

EXHIBIT 1

**MONEY SERVICES, INC.
PROFESSIONAL SERVICES AGREEMENT**

This Professional Services Agreement ("Agreement") is entered into as of the 1st day of April, 2014 (the "Effective Date"), by and between Money Services, Inc. ("Company") located at 4333 Edgewood Road, Cedar Rapids, Iowa 52499 and Examination Management Services, Inc. ("Service Provider") located at 3050 Regent Boulevard, Suite 400, Irving, Texas 75063.

WHEREAS, Company desires to retain Service Provider to provide Services related to the Services defined in Exhibit C and Exhibit D herein for Company Affiliates, and Service Provider is willing to provide such Services subject to the terms of this Agreement;

WHEREAS, Company possesses certain confidential and/or proprietary information and in connection with the Services, Company confidential and/or proprietary information will become available or disclosed to, or will be generated by, Service Provider, and Company desires to prevent the unauthorized use and disclosure of such confidential and/or proprietary information;

WHEREAS, in addition to the Services contemplated by the parties, Service Provider may also provide information technology services or other Deliverables related to the provision of Services;

WHEREAS, privacy requirements have been enacted into law pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as well as other state and federal laws, which requirements impose on Company the obligation to enter into a Business Associate Agreement for some of the Services; and

WHEREAS, as a result of the Services and access to confidential and/or proprietary information, Service Provider may design, create, invent or initiate further proprietary information and Company and Service Provider desire that such proprietary information shall belong to Company.

NOW, THEREFORE, in consideration of the covenants set forth herein, and for other good and valuable consideration, the receipt, adequacy and sufficiency of which is hereby acknowledged, the parties agree as follows:

1. **DEFINITIONS.** The following terms have the meanings ascribed to them when used in this Agreement or in any Statement of Work. Other terms, when capitalized, have the meanings defined elsewhere in this Agreement.

1.1 An "**Affiliate**" of a specified Person is a Person that directly or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with, the Person specified. For the purpose of this definition, the term "control" (including the terms "controlling," "controlled by" and "under common control with") means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a Person, whether through the ownership of voting securities, by contract, or otherwise.

1.2 "**Applicable Laws**" means all applicable conventions, laws, rules, regulations and orders of governmental authorities having jurisdiction over the subject matters of this Agreement, including without limitation, state and federal anti-kickback and anti-referral laws and regulations.

1.3 "**Change Order**" is defined in Section 3.10.

1.4 "**Confidential Information**" shall mean information identified on, in or constituting: all strategic and development plans, financial information, results of the Services, business plans, information about the Disclosing Party and/or its Affiliates, co-developer identities, data, business records, customer lists, policy information, personally identifiable information, personal financial information or personal health information (as those terms are defined by governing law), product designs, test data, project records, market reports, investor information, know-how, discoveries, ideas, concepts, specifications, models, diagrams, methodologies, research, technical and statistical data, drawings, models, flow charts, work-flow, marketing, pricing, selling, distribution, database descriptions, software code, source code, object code, Intellectual Property, and any and all other tangible or intangible information, other than Trade Secrets, encompassed in any medium, which may be disclosed, whether or not in writing, whether or not marked as "Confidential" or "Proprietary" by the Disclosing Party or to which the

Receiving Party may be provided access to by Disclosing Party in accordance with this Agreement, or which is generated or learned as a result of or in connection with the Services and is not generally available to the public. "Confidential Information" also includes proprietary or confidential information of any third party that may disclose such information to either party in the course of the third party's relationship with such party. For clarification purposes, Confidential Information includes Nonpublic Personal Financial Information, Protected Health Information, and Electronic Protected Health Information.

1.5 **Cure Period**" is defined in Section 7.2.

1.6 **Deliverables**" means the Services and tangible items that are specified in and provided to Company pursuant to a Statement of Work issued under this Agreement and includes, without limitation, any materials, documentation, designs, drawings, data files, computer programs, textual items, audio and visual items, graphical items and modifications thereto (including both source code and object code) and other works of authorship resulting from the performance of Services under this Agreement by Service Provider, its agents and subcontractors, whether fixed in digital, magnetic or optical media or document form.

1.7 **DHHS**" means the United States' Department of Health and Human Services.

1.8 **Disclosing Party**" is defined in Section 5.5.

1.9 **Electronic Protected Health Information**" or "**ePHI**" means any information that: (A) relates to the past, present, or future physical or mental health or condition of a Policyholder, the provision of health care to a Policyholder, or the past, present or future payment for the provision of health care to a Policyholder; (B) that identifies a Policyholder, or with respect to which there is a reasonable basis to believe the information can be used to identify the Policyholder; and (C) that is transmitted by electronic media or maintained in electronic media and as further defined within 45 CFR 160.103 (as amended or superseded from time to time).

1.10 **Force Majeure**" means any act or event, whether foreseen or unforeseen, that meets all three of the following:

- (a) The act or event prevents the nonperforming party, in whole or in part, from:
 - (i) performing its obligations under this Agreement; or
 - (ii) satisfying any conditions to the performing party's obligations under this Agreement.
- (b) The act or event is beyond the reasonable control of and not the fault of the nonperforming party.
- (c) The nonperforming party has been unable to avoid or overcome the act or event by the exercise of due diligence;

provided, however, that, notwithstanding (a), (b) and (c) above and in any event, Force Majeure excludes economic hardship, labor strikes or shortages, changes in market conditions or insufficiency of funds.

1.11 **HIPAA Covered Products**" means any insurance products offered by Company or any of its Affiliates which are subject to HIPAA and/or HITECH, as amended from time to time.

1.12 **Implementation Schedule**" means a schedule set forth in a Statement of Work for the delivery or implementation of one or more Deliverables to which the Statement of Work pertains, listing "milestones" based on key occurrences, such as the development of Specifications, delivery of items for testing, completion of tests and the like.

1.13 **Intellectual Property**" means any and all now known or hereafter known or developed tangible and intangible: (a) rights associated with works of authorship throughout the universe, including, but not limited to, copyrights, moral rights and mask works; (b) trademarks, service marks, trade names and any other indicia of origin; (c) Trade Secrets; (d) patents, pending patent applications, designs, algorithms and other industrial property rights; (e) all other intellectual and industrial property rights (of every kind and nature throughout the universe and however designated, including "rental" rights and rights to remuneration), whether arising by operation of law, contract, license or otherwise; and (f) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues now or hereafter in force (including any rights in any of the foregoing).

1.14 “**Nonpublic Personal Financial Information**” means personally identifiable financial information about Policyholders and includes, without limitation, any list, description, or other grouping of Policyholders (and publicly available information pertaining to them) that is derived using any nonpublic personal information; provided, however, that the above definition shall be superseded and replaced to the extent that the definition of Nonpublic Personal Financial Information under Title V of Public Law 106-102, Section 509, subsection (4) (as amended or superseded from time to time) differs therefrom.

1.15 “**Person**” shall be construed as broadly as possible and shall include, without limitation, any natural person, corporation, partnership, limited partnership, limited liability company, trust, group, association or other entity.

1.16 “**Policyholder**” means any individual or entity who presently or in the past has applied for, owned or been covered by a product offered by Company or its Affiliates.

1.17 “**Policy**” and “**Policies**” means insurance policies or certificates of insurance coverage issued by Company or its Affiliates.

1.18 “**Proprietary Information**” means Confidential Information and Trade Secrets, whether in written, oral, electronic or other form, furnished, transmitted to, observed or obtained by one of the parties (including, without limitation, any Confidential Information or Trade Secrets that are in a party’s facility and are viewable, accessible or otherwise made available to Receiving Party); provided, however, that, to the extent reasonably substantiated by documentation, the following information is not Proprietary Information and Receiving Party is not restricted as to its use or disclosure:

- (a) information already in the possession of, or already known to, the Receiving Party as of the Effective Date, and not under any other obligations of confidentiality due to any other agreements between the parties;
- (b) information that enters the public domain after the Effective Date, or which, after such disclosure, enters the public domain through no fault of the Receiving Party;
- (c) information lawfully furnished or disclosed to the Receiving Party by a non-party to this Agreement without any obligation of confidentiality;
- (d) information independently developed by any party without use of any Proprietary or Confidential Information; or
- (e) information that is explicitly approved for release by the Disclosing Party.

1.19 “**Protected Health Information**” or “**PHI**” shall have the same meaning as the term “protected health information” in 45 C.F.R. §164.501 (as amended or superseded from time to time), limited to information created or received by Service Provider or its affiliates from or on behalf of Company and its Affiliates, or otherwise created or received by Service Provider, and shall include, without limitation, any and all information that relates to the past, present, or future physical or mental health or condition of a Policyholder, to the provision of health care to a Policyholder, or to the past, present, or future payment for the provision of health care to a Policyholder, and that identifies Policyholder or for which there is a reasonable basis to believe that the information can be used to identify the Policyholder, in each case regardless of whether the Policyholder is living or deceased. By way of illustration only, the following information shall constitute Protected Health Information with respect to a Policyholder: (i) name, (ii) street address, city, county, precinct, and zip code, (iii) dates directly related to the Policyholder, including birth date, (iv) telephone numbers, fax numbers, and electronic mail addresses, (v) social security number, (vi) policy or certificate number, and (vii) any other unique identifying numbers, characteristics, or codes. Such information shall constitute Protected Health Information regardless of whether it is in electronic, paper, or any other format.

1.20 “**Receiving Party**” is defined in Section 5.5.

1.21 “**Representative**” means any director, officer, employee, agent, representative, advisor or consultant of either of the parties or any director, officer, employee, agent, representative, advisor or consultant of an Affiliate. The term “Representative,” when used with respect to Service Provider, shall include such Subcontractors and their respective directors, officers, employees, agents, representatives, advisors and consultants.

1.22 “**Self-Help Code**” means any back door, time bomb, trap door, drop dead device, or other software routine designed to disable a computer program automatically with the passage of time or under the positive control of a person other than a user of the program. Self-Help Code does not include software routines in a computer program, if any, designed to permit an owner of the computer program (or other person acting by authority of the owner) to obtain access to a user’s computer system(s) (e.g., remote access via modem) for purposes of maintenance or technical, or other purposes indicated in the applicable software’s documentation.

1.23 “**Services**” mean all Services to be furnished to Company by Service Provider or its subcontractors as set forth in an applicable Statement of Work.

1.24 “**Specifications**” mean the functional and operating specifications and requirements of any Deliverable, as set forth in an applicable Statement of Work.

1.25 “**Statement of Work**” means a written instrument that meets the requirements of Section 3, and is executed by the authorized representatives of both parties for the performance of Services or the creation of Deliverables and which shall, once executed, form an integral part of this Agreement.

1.26 “**Term**” is defined in Section 9.1.

1.27 “**Trade Secrets**” mean technical and non-technical information (regardless of whether such information is in tangible or intangible form) including source code, object code, computer code, data, ideas, concepts, formulae, methods, techniques, processes, financial business plans and business methods (including any derivatives of any of the foregoing) disclosed to either party by or on behalf of the other party that derive economic value, actual or potential, from not being generally known to other persons who could obtain economic value from the disclosure or use thereof, and which are the subject of efforts that are reasonable under the circumstances to maintain their secrecy.

1.28 “**Unauthorized Code**” means any virus, salamis, Trojan horse, Easter eggs, logic bomb, worm, programs or computer instructions that self-replicate without manual intervention, or other software routines or hardware components designed to permit unauthorized access, disable, erase, or otherwise harm software, hardware, or data, or to perform any other unauthorized actions. The term Unauthorized Code does not include Self-Help Code.

1.29 “**Virus**” means any computer instructions designed to disrupt, disable, harm, alter, destroy or otherwise impede in any manner, including aesthetical disruptions or distortions, the operation of the Software, or any other software, data storage, computer libraries, firmware, hardware or computer system (including local area or wide-area networks). Viruses include, but are not limited to, Self-Help Code and Unauthorized Code.

2. **RELATIONSHIP OF PARTIES.**

2.1 **Independent Contractor.**

(a) **Service Provider as Independent Contractor.** Service Provider agrees and acknowledges that Service Provider is an independent contractor under this Agreement, with the authority to control the manner, method and means of Service Provider’s performance. Company shall inform Service Provider only of the results it desires, the completion date, and assessment of the Services to ensure they have been performed in accordance with Service Provider’s engagement. Personnel supplied by Service Provider hereunder are not employees or agents or Company or its Affiliates and Service Provider assumes full responsibilities for their acts. Nothing contained in this Agreement shall be deemed or construed to create an employer/employee relationship or any partnership or joint venture between Service Provider and Company. Service Provider acknowledges and agrees that only eligible employees of Company are entitled to benefits under Company (i) pension and welfare plans (as the Employment Retirement Income Security Act defines those terms) and (ii) any other benefit arrangements, and that Service Provider’s status as an independent contractor makes Service Provider ineligible to participate in these plans and arrangements. Service Provider shall not at any time hold itself out as an employee of Company. The parties shall not make any commitments or incur any charges or expenses for or in the name of one another and shall, to the greatest extent possible, perform this Agreement in a manner consistent with Service Provider’s status as an independent contractor.

(b) Subcontractors. Service Provider may subcontract with another person or entity (each a "Subcontractor") for the performance of some or all the Services; provided, however, that no subcontract shall relieve Service Provider from any obligations or liabilities hereunder and Service Provider shall remain responsible for all obligations or liabilities of each Subcontractor with respect to provision the Services as if provided by Service Provider. Service Provider shall cause each Subcontractor and its employees, agents, and representatives to comply with the terms and conditions of this Agreement applicable to them. Service Provider shall, at the request of Company in its sole reasonable discretion, cease using any Subcontractor to Service the Company or its Affiliates.

2.2 Administration of Contract.

(a) Personnel.

(i) Qualifications. Service Provider shall provide individuals who are duly qualified and skilled in the area in which their Services are to be utilized ("Placed Personnel"). Company possesses the right to reasonably reject any individual so furnished, if dissatisfied with such individual's performance. If any Placed Personnel is rejected, Service Provider agrees to use commercially reasonable efforts to furnish a suitable replacement within a reasonable time.

(ii) Reassignment. Service Provider shall use commercially reasonable efforts to adhere to applicable staffing plans to meet forecasted support requests. If any personnel change occurs, Service Provider shall adhere to schedules, absorb costs of any unavoidable duplication or retraining, and assure that personnel of at least comparable qualifications and experience are assigned to complete the Services and are reasonably satisfactory to Company.

(iii) Drug and Background Screens. Service Provider agrees to notify its Placed Personnel who perform Services under this Agreement of the Service Provider's policy concerning drug and alcohol use that prohibits (A) the use, possession, distribution, purchase or sale of drugs or alcohol on Company's premises or while engaged in Service Provider's business and (B) reporting to or performing work for Company while under the influence of drugs or alcohol (except for authorized amounts of over-the-counter or prescribed drugs required for health reasons). Further, Service Provider agrees that its policy will allow Service Provider:

- a. to screen any Placed Personnel for the unauthorized or unlawful use of drugs by having Placed Personnel submit to a licensed laboratory for screening or be terminated. Service Provider further agrees to confirm that any Placed Personnel did not engage in the unauthorized or unlawful use of drugs at the time of such screen. If Service Provider cannot confirm such, Service Provider shall promptly remove such Placed Personnel and replace him or her with replacement personnel with substantially the equivalent or better qualifications within seven (7) days.
- b. to conduct a background investigation that will confirm that the Placed Personnel has not been convicted of a felony involving theft, dishonesty, or breach of trust, or any provision of the Federal Crime Bill. If Service Provider cannot confirm such within thirty (30) days of placement of the Placed Personnel, Service Provider shall immediately remove Placed Personnel and replace him or her with replacement personnel with substantially the equivalent or better qualifications within seven (7) days.

(iv) Compliance with Laws. Service Provider represents and warrants that in the course of providing Services under this Agreement that Service Provider shall comply with all applicable federal, state and local laws, rules, regulations, ordinances, codes, orders and/or programs. Service Provider further represents and warrants that it will have obtained any necessary permits, licenses or any other documentation and authorization required to comply with any such laws and regulations. Service Provider hereby certifies that it shall fully comply with Executive Order 11246, as amended by Executive Order 11375, Section 503 of the Rehabilitation Act of 1973, as amended, the Vietnam War Veteran Readjustment Assistance Act of 1974, as amended, Executive Order 11625, as amended and the rules and regulations issued thereunder, any privacy laws, the Fair Labor Standards Act, the Equal Pay Act, the Occupational Safety and Health Act, Americans with Disabilities Act, The Age Discrimination in Employment Act, Title VII of the Civil Rights Act, Immigration and Control Act,

Family and Medical Leave Act, and provisions relating to the identification and procurement of required permits, certificates, approvals and inspections, labor and employment obligations, affirmative action, and wage and hour laws, which are hereby incorporated by reference as appropriate. Service Provider commits itself to such compliance by entering into this Agreement. Service Provider shall require its applicable subcontractors to comply with this Section.

(b) **Access to Premises.** Company agrees to provide Service Provider with physical access to premises under the control of Company as may be necessary for Service Provider to perform its obligations under this Agreement. Company agrees to arrange such security clearances as may be required in order to provide such physical access. Service Provider shall ensure that its employees, agents, and subcontractors at all times comply with all applicable federal, state, county, local laws in the performance of the Services. Further, Service Provider will comply with this Agreement and applicable facility rules. Service Provider recognizes that its access to and usage of Company's resources such as, but not limited to, office equipment and supplies, computer network, software and hardware, data/voice/image storage and transmission are intended for authorized Company business use only and Service Provider and its personnel may be held personally responsible for any unauthorized use or disclosure. Service Provider shall use any such resources, including software, network and computer equipment only in connection with the performance of the Services. Service Provider recognizes that Company does not and cannot guarantee the privacy of files, information and messages stored in Company-owned files, desks, storage areas, or electronic media. For various reasons including maintenance, security, business, legal, compliance or regulatory requirements, authorized Company personnel must have unrestricted access to information stored in or on Company property or equipment. Any original documents, electronic records, files or records (including building access badges) which Company provides to Service Provider are and shall remain the sole property of Company. Service Provider shall return or destroy such property to Company within thirty (30) days after receiving Company's request and after the earlier of the termination of this Agreement or any individual Statement of Work.

2.3 **Company Subsidiary, Company Affiliate and Division Participation.** Company acts on behalf of itself and for its Affiliated member companies and divisions of such member companies, all of which are part of the AEGON Group (for purposes of this Section only, "Company Affiliate"). Company reserves the right to extend the benefits, obligations and privileges of this Agreement to each Company Affiliate even though each such Company Affiliate is not specifically named as a party to this Agreement. Each such Company Affiliate may execute a separate Statement of Work for Services, subject to the terms and conditions of this Agreement, and all such terms and conditions applying to Company shall apply to the Company Affiliate as if it was an original party to this Agreement, in which event: (i) the agreement between Service Provider and such Company Affiliate shall consist collectively of this Agreement and the Statements of Work(s) between Service Provider and such Company Affiliate, and (ii) such agreement shall constitute a separate, bilateral professional services agreement between Service Provider and such Company Affiliate. Further, each such Company Affiliate shall be individually responsible for its own payment and any obligation incurred under this Agreement. The failure of one Company Affiliate to satisfy its obligations under this Agreement shall in no way affect the performance or obligations between Service Provider and any other participating Company Affiliate, and the obligations of Company and such Company Affiliates to Service Provider shall in all events be several, and not joint and several.

3. **SERVICES**

3.1 **Services.** Service Provider shall provide Services under this Agreement in accordance with the applicable Statement of Work(s) agreed to by the parties and issued hereunder.

3.2 **Statement of Work.** All Services to be performed hereunder are to be specifically identified in Statements of Work as described herein. A separate Statement of Work will be prepared for each significant project mutually agreed to be undertaken in connection with this Agreement. Services performed in connection with any Statement of Work are deemed to be Services performed in connection with this Agreement. A template Statement of Work is attached as Exhibit A.

3.3 **Contents.** Except for minor tasks, which may be addressed in summary form, each Statement of Work may generally contain the following items:

- (a) A detailed description and/or Specifications of the Services to be performed and the Deliverables;
- (b) Completion and acceptance criteria to be applied in order to confirm that any Deliverables and/or Services meet the applicable Specifications;
- (c) A description of any work, Services or other items to be provided by Company or Service Provider;
- (d) The identity of, and contact information for, a project manager for each of Service Provider and Company (collectively "Project Managers");
- (e) The amount, schedule and method of payment;
- (f) An Implementation Schedule setting forth a timetable for delivery of Deliverables, acceptance testing, acceptance and other key milestones;
- (g) The term of the Statement of Work;
- (h) Such other terms and conditions as may be mutually agreeable between the parties; or
- (i) Any resources each party will provide.

3.4 **Adoption of Statement of Works and Changes.** Each Statement of Work will be effective only if in writing, approved, and signed by each party.

3.5 **Formalities.** Each Statement of Work shall reference this Agreement. The contents of the Statement of Work may be included in the body of the Statement of Work, or in separately signed attachments, as the parties consider most practical. It may also refer to or incorporate by reference other documentation that has been separately signed by the parties, such as all or a portion of any other Statement of Work that the parties have adopted. Each Statement of Work and changes to a Statement of Work are to be effective only if in writing accompanied by dated signatures of officers of each party. Service Provider is not authorized to provide to Company or to commit Company to procure any Services except in accordance with a signed Statement of Work.

3.6 **Project Managers.** The parties' Project Managers designated in a Statement of Work are responsible for:
(a) arranging all meetings, visits and consultations between the parties about such Statement of Work;
(b) receiving all notices and reports about such Statement of Work; and
(c) all administrative matters such as processing of invoices, payments, amendments and change orders to a Statement of Work.

3.7 **Modes of Payment.** Modes of payment for all Services and Deliverables shall be set forth in each Statement of Work or Exhibit D attached hereto. The rates stated in Exhibit D shall be effective for two (2) years from the Effective Date. Unless otherwise notified by Company at least thirty (30) days before the end of the then current term, this Agreement shall renew automatically for an additional one (1) year term at the then current term, plus any increase in fees agreed to in writing by the parties. If Service Provider is unwilling to renew this Agreement at the rates then in effect, it must notify Company at least sixty (60) days before the end of the then-current term of any proposed price increase. Any price increase after the first two (2) years shall be limited to the annual increase in the prior year's Consumer Price Index-Core (CPI) Index as published monthly by the Bureau of Labor Statistics, US Department of Labor or 3%, whichever is lesser.

3.8 **Implementation Schedules.** Service Provider shall use all commercially reasonable efforts to complete the Services and Deliverables according to the Implementation Schedule. Service Provider shall also prepare and submit such further reports of its performance and progress as Company may reasonably request from time to time.

3.9 **Incorporation of this Agreement by Reference; Precedence.** Each Statement of Work is deemed to incorporate the terms and conditions of this Agreement by reference. In the event of any express conflict or inconsistency between the provisions of a Statement of Work and the provisions of this Agreement, this Agreement controls unless the Statement of Work explicitly identifies the section of this Agreement that is superseded by the Statement of Work. Any change to a Statement of Work that follows the requirements of this Section will only apply to that Statement of Work.

3.10 **Change Orders.**
(a) **Right to Request Changes.** Either party may propose to reduce, alter, amend, enhance, or add to the scope or nature of the Deliverables to be provided under this Agreement or any Statement of Work or to modify the time or place of performance hereunder.

(b) **Procedure.** If either party proposes a change in a Statement of Work, such party shall provide a written change order ("Change Order") to the Project Manager of the other party. The request must be clearly identified as a proposal or request for a Change Order and provide information regarding the change comparable to the detail originally included in the applicable Statement of Work, including a description of the anticipated impact on the Services to be performed. If Company proposes a change, then within ten (10) business days after Service Provider's receipt of the proposal from Company, Service Provider shall advise Company of pricing or other terms that Service Provider believes will be affected by the proposed changes. Only a material change in a Statement of Work may result in a pricing change. If the proposed terms are not acceptable to Company, Service Provider and Company shall endeavor to agree upon appropriate and mutually agreeable changes in price, timing or other terms associated with the Change Order. If Service Provider and Company cannot agree upon such changes within twenty (20) business days after Service Provider's receipt of the notice of proposed changes from Company, the Services will continue with no change. While such changes are under review, Service Provider shall continue to perform the Services. Service Provider agrees to act in a commercially reasonable manner with regard to terms it requires for any proposed change. Service Provider shall evaluate proposed Change Orders at no additional charge to Company.

(c) **Right of Refusal.** Service Provider may not decline any Change Order that increases the cost or magnitude of performance, provided that the changes are reasonable in scope and a commensurate increase in compensation is fixed. Except as otherwise provided in this Agreement, neither party will be obligated to agree to any change in the Services and the provisions of this Section 3.10 set forth the only manner in which such changes to the Services may be accomplished. Each party agrees to act in good faith with respect to changes proposed by the other party.

3.11 **Reports.** Without limiting Service Provider obligations elsewhere in this Agreement, Service Provider will provide Company and its Affiliates with access to secure web based reports and statistical information with respect to Service Provider performance of the Services as Service Provider and/or Company or its Affiliates may reasonably deem necessary to apprise Company and its Affiliates adequately of Service Provider performance of the Services.

3.12 **Communications.**
(a) **Representations about Company and its Affiliates.** Service Provider hereby acknowledges that Company and its Affiliates are regulated by many governmental authorities ("Governmental Authorities"), and that performance hereunder may be subject to laws, regulations and policies enforced by Governmental Authorities. Neither Service Provider nor any of its Representatives shall make any oral or written representation relating in any way to Company and/or its Affiliates to any Governmental Authorities.
(b) **Representations about the Policies.** Service Provider shall not make any representations or other statements of any kind to Policyholders or any other person about the Policies, the coverage provided under the Policies or any of them, or any Policyholder's eligibility for benefits under a Policy.

3.13 **Nondiscrimination.** Service Provider will not discriminate because of age, sex, race, religion, color or national origin in its operations and provision of Services to any Policyholder.

3.14 **No Preferred Provider Arrangement.** Service Provider, in its performance of Services, is not and does not constitute a preferred provider arrangement, preferred provider organization, health maintenance organization, managed care plan or similar plan, network or arrangement.

3.15 **Books and Records.** Service Provider shall maintain or cause to be maintained those books, data, records and files required to reflect the Services (collectively, the "Records") in accordance with Supplier's policies or such longer period as required under applicable law. Company and its Affiliates shall have the right to inspect and audit Service Provider, Records during normal business hours by providing notice to Service Provider at least thirty (30) days prior to the date of the inspection or audit. Those Governmental Authorities exercising authority over Company and/or its Affiliates similarly shall have access to the Records as may be required by law or reasonably requested by Company and/or its Affiliates, and/or the Governmental Authorities.

3.16 **Lawsuits and Other Claims.** Service Provider shall notify Company and its Affiliates in writing within three (3) business days after Service Provider becomes aware of: (i) the institution or commencement of any claim, cause of action, suit, investigation or proceeding (including without limitation a disciplinary proceeding instituted or commenced by any Governmental Authority) in connection with Service Provider performance of the Services or any other obligation under this Agreement, or (ii) any communication threatening litigation against Service Provider and/or Company and/or its Affiliates in connection with Service Provider performance under this Agreement.

3.17 **Disposal and Destruction of Proprietary Information.** Service Provider agrees to comply at all times with Company's reasonable requests for disposal and destruction of any of Company's Proprietary Information, including, but not limited to, the following guidelines for:

- (a) Prior to destruction, all Proprietary Information will be secured against unauthorized access;
- (b) Proprietary Information on Film: physical destruction through chemical, melting, incineration, or shredding with cross cut - no larger than 5/32" x 4/5";
- (c) Proprietary Information on Magnetic Media or Solid State: bulk erase (except for hard drives) through destructive write or secure deletion/erasure;
- (d) Proprietary Information on Magnetic Media or Solid State: physical destruction through hammer mill, shredding, or overwrite with high values (binary 1's), low values (binary 0's), or random bit patterns; and
- (e) Proprietary Information on Optical Media: physical destruction through incineration, melting, or shredding.

4. **FEES AND PAYMENTS**

4.1 **Fees.** In consideration for providing Services hereunder, Company shall pay in U.S. dollars to Service Provider the Service Fees pursuant to the terms set forth herein and in each applicable Exhibit or Statement of Work. Except as otherwise agreed in writing by both parties, the payment described in a Statement of Work is to be the sole compensation to Service Provider for the performance of Services thereunder.

4.2 **Invoices and Payment.** Service Provider shall invoice Company for the prices, charges, taxes and reimbursable items payable to Service Provider as the conditions to payment are satisfied, with such supporting documentation as Company reasonably requests. If the invoice is valid and undisputed, Company shall pay the invoiced amount by the 30th day following receipt, unless a different time for payment is described in the Statement of Work. Invoices are to be addressed to the appropriate underwriting area for payment as defined by Company. Each invoice is to provide in reasonable detail the particular Services performed. Any extraneous terms on Service Provider's invoices are void and of no effect. In the event of any good faith dispute with regard to a portion of an invoice, the undisputed portion is to be paid according to the procedures described in this Section 4.2.

4.3 **Expenses.** In the event that a Statement of Work provides for the reimbursement of Service Provider's expenses in connection with performing Services thereunder, such reimbursement is limited to actual out-of-pocket expenses reasonably incurred that are pre-approved by Company in an Exhibit or Statement of Work, including travel expenses (e.g., airfare, local transportation, lodging and meals) and miscellaneous expenses (e.g., reproduction and shipping costs of materials). Service Provider shall provide a concrete plan for managing such costs. All expenses, including per diem expenses, are to be in accordance with Company's generally applicable policies (at actual cost to Service Provider) and must be approved in advance. Air travel is to be by coach or economy class only. Service Provider's policies for reimbursement of employee or contractor travel and living expenses are subject to Company's review and approval. Upon reasonable request, Service Provider shall provide Company with supporting documentation (such as receipts for travel, hotels and rental cars) with regard to such reimbursable expenses. Service Provider agrees to use the same diligence in controlling reimbursable expenses as it uses in its own business for expenses incurred by Service Provider, but in no event is Service Provider to use less than commercially reasonable diligence.

4.4 **No Other Payment.** Except as expressly provided in this Agreement or the applicable Statement of Work, Service Provider and Company shall each bear all of its own expenses arising from the performance of its

obligations under this Agreement, including, without limitation, personnel, facilities, utilities, equipment, supplies, clerical and the like.

4.5 **Annual Review of Fees.** The parties shall review all amounts due under this Agreement at least annually.

4.6 **Adjustment for Errors.** All payments made under this Agreement are subject to adjustment in the event of an error affecting such payment. Appropriate adjustments will be made within thirty (30) days after receipt of written notice of the error.

5. **PROPRIETARY RIGHTS/CONFIDENTIALITY/PRIVACY/SECURITY BREACH**

5.1 **Company Ownership of Deliverables.** Company shall have sole ownership of all right, title and interest in any Deliverables produced by Service Provider and its Representatives as a result of the Services performed under this Agreement. Service Provider agrees that any and all Deliverables produced by Consultant hereunder belong exclusively to Company and are Company Proprietary Information.

5.2 **Assignment of Intellectual Property Rights.**

(a) **Works for Hire.** All Deliverables are deemed works for hire. To the extent that any Deliverables may not, by operation of law, be works made for hire, Service Provider hereby irrevocably assigns to Company, and to the extent applicable shall require its Representatives to assign to Company, all patent, copyright and other proprietary rights of any kind in, to and under the Deliverables. Except as provided below in Sections 5.3 or 5.5, no rights are reserved for Service Provider.

5.3 **Ownership of Pre-existing Works.** Service Provider retains ownership of any pre-existing software or work of authorship which is incorporated into the Deliverables provided to Company hereunder, but with respect to such pre-existing software or works of authorship which are not otherwise licensed to Company under other agreements, Service Provider hereby grants to Company a royalty free, non-exclusive, perpetual, sub-licensable license to use, modify or create derivative works of such pre-existing software or works of authorship in connection with Company's use of the Deliverables. Any pre-existing software or works of authorship must be identified in the applicable Statement of Work for ownership to remain with Service Provider.

5.4 **"INTENTIONALLY DELETED"**

5.5 **Proprietary/Confidential Information.**

(a) **Protection of Proprietary Information.** If Proprietary Information is disclosed to a party ("Receiving Party") by the other party ("Disclosing Party"), then Receiving Party agrees that it shall hold such Proprietary Information in confidence, agrees not to disclose any Proprietary Information to persons not having a need to know such Proprietary Information consistent with the purpose for which it was transmitted and such Proprietary Information will not be used, directly or indirectly, for any nonprofit, commercial, business or other purpose or in any way detrimental to Disclosing Party. Receiving Party shall take reasonable precautions to protect the confidentiality and value of Proprietary Information to Disclosing Party including measures to prevent loss, theft and misuse. Receiving Party shall give notice to Disclosing Party of any unauthorized use or disclosure of Proprietary Information, as soon as reasonably practicable. Receiving Party agrees to assist Disclosing Party in remediating any unauthorized use or disclosure of Proprietary Information caused by such Receiving Party.

(b) **Protection of Policyholder Confidential Information by Service Provider.** Except to the extent directly required to perform a legal duty, its obligations under this Agreement or as otherwise specifically authorized in writing by Company and its Affiliates or the Policyholder to whom such information relates, Service Provider shall hold in strictest confidence and not disclose to any Person at any time, whether during or after the term of this Agreement any Confidential Information in any form, whether, written, oral or electronic, directly or indirectly related to Policyholders. Service Provider shall apply at least the same standard of care to protect the confidentiality of Confidential Information as it uses to protect its own confidential information. Service Provider shall not use Confidential Information for any purpose except to the extent specifically provided for in this Agreement.

(c) **Provision of Policyholder Confidential Information to Service Provider.** Company and its Affiliates may provide Service Provider with Policyholder Confidential Information reasonably necessary to the provision of the Services.

(d) **Business/Regulatory Record Exception.** Each party acknowledges the information contained in notes, correspondence and reports prepared by a party in connection with the party's discussions are business records of the Receiving Party. Each party agrees that business records and Proprietary Information retained for any regulatory requirement or as part of an automatic journaling or retention system need not be returned or destroyed, but are subject to all other terms of this Agreement.

(e) **Return of Proprietary Information.** Upon written request of a party, each party shall promptly as possible (and in any event within thirty (30) days) return or destroy (as directed by the Disclosing Party) all Proprietary Information received from the other party, including all copies, except to the extent such return or destruction is not feasible, and except Proprietary Information Receiving Party is entitled to retain under Section 5.5(d). Upon the request of the Disclosing Party, the Receiving Party shall furnish to the Disclosing Party an affidavit providing assurances as to the return or destruction of the Disclosing Party's Proprietary Information.

(f) **Disclosure Required by Law.** In the event that Service Provider receives a request to disclose all or any Proprietary Information under the terms of a subpoena or order issued by a valid court or other governmental body (including without limitation any department of insurance), or any other request for disclosure of Proprietary Information, Service Provider agrees, if permitted by Applicable Law: (i) to notify Company as soon as reasonably practicable after Service Provider receives the request, and in any event prior to responding thereto, of the existence, terms and circumstances surrounding such request; (ii) to consult with Company on the advisability of taking legally-available steps to resist or narrow such request; and (iii) if disclosure of Proprietary Information is required to prevent Service Provider from being held in contempt or subject to other penalty, to furnish only such Proprietary Information as Service Provider is advised by outside counsel that it is legally compelled to disclose and to exercise its best reasonable efforts to obtain assurance that confidential treatment will be accorded to the disclosed Proprietary Information.

(g) **HIPAA Covered Products.** Service Provider and its Representatives shall comply with (a) all Applicable Law respecting the confidentiality of Policyholder information and data concerning Policyholders acquired in the course of Service Provider performance of its obligations under this Agreement, including, but not limited to, HIPAA and regulations promulgated thereunder, and (b) with other confidentiality provisions set forth in this Agreement.

5.6 Prohibition of Use of Company Name and Trademarks. Each party shall not use the name, trademark, trade dress, logo or other indicia of origin of the other party or any Affiliate of the other party (collectively, "Name") in advertising or sales materials or in any other manner whatsoever without prior express written approval of the party owning such Name, except in furtherance of performing Services or satisfying legal duties. Such prohibition includes, without limitation, the following:

- (a) Each party shall not refer to the existence of this Agreement without the other party's prior express written approval;
- (b) Each party's use of the other party's Name is strictly limited to meeting disclosure obligations imposed by regulatory bodies, such as the SEC or FINRA;
- (c) Each party is not allowed to make any statement or representation whatsoever regarding the other party's company, product or services without the first party's prior express written approval; and
- (d) If a party provides prior express written approval for the use of its Name, such party further reserves the right to revoke such approval at any time.

5.7 Ownership. Except as provided in this Agreement or any Statement of Work, all materials transmitted between the parties are to remain the sole and exclusive property of the Disclosing Party to the extent that they contain Proprietary Information. Except for the licenses or ownership rights granted in this Agreement, this Agreement and transmission or disclosure of any Proprietary Information does not grant the Receiving Party a license or ownership of any type.

5.8 Expiration of Obligations. All obligations and restrictions of confidentiality under this Agreement are to remain in effect for a period of seven (7) years following the date of disclosure for Confidential Information, and with respect to Trade Secrets pursuant to applicable law, for as long as such information remains a Trade Secret. All obligations of confidentiality and all restrictions on the use of Personal Information and Protected Health

Information under this Agreement are to remain in effect for as long as such information remains Personal Information (as that term is defined in Section 5.11) or Protected Health Information. Such time periods may be extended upon written agreement of the parties.

5.9 **Responsibility for Affiliates and Representatives.** Each party is solely responsible for any breach of this Agreement by its Representatives including, without limitation, any improper use or disclosure by its Representatives of the other party's Proprietary Information. Receiving Party may disclose Proprietary Information to its Representatives who in Receiving Party's reasonable judgment have the need to know such information in connection with this Agreement. Receiving Party shall inform its Representatives of the confidential nature of such Proprietary Information, shall direct them to hold Proprietary Information in strict confidence, shall take all reasonable precautions to prevent improper use of Proprietary Information by them, and shall be responsible for any breaches by them of the terms found in this Agreement.

5.10 **Proprietary Legends.** Neither party shall remove or obscure the proprietary legends or marks appearing on materials provided by the other party.

5.11 **Privacy.**

For purposes of Sections 5.11, 5.12 and 5.13 only, the following definitions shall apply:

"Applicable Privacy Law" means any law, ordinance, statute, rule or regulation applicable to or binding on either party with respect to privacy or data security, including but not limited to the Health Insurance Portability and Accountability Act of 1996 "HIPAA" and all related regulations issued pursuant to the Act, the Health Information Technology for Electronic and Clinical Health Act ("HITECH") and all related regulations issued pursuant to the Act, the Gramm-Leach-Bliley Act (Pub. L. 106-102) ("GLBA"), Regulation S-P (17 CFR 248), the Fair and Accurate Credit Transactions Act of 2003 (Pub. L. 108-159), and the Standards for the Protection of Personal Information of Residents of the Commonwealth of Massachusetts (210 CMR 17), as each may be amended from time to time.

"Personal Information" means, in addition to any definition under Applicable Privacy Law, any personally identifiable information about any individual, including, but not limited to, name, email address, telephone number, age or date of birth, gender, zip code, demographic information, marketing preferences, social security number, alien identification number, credit or debit card numbers, other financial account numbers, application data, credit history, financial information, drivers license number, other unique identifier or authenticator, health insurance or medical information, consumer report information and data about transactions or experiences with Company or marketing partner of Company. The term "individual" for purposes of this definition includes, but is not limited to a customer, client, employee or contractor of Company. Personal Information includes Nonpublic Personal Financial Information, Electronic Protected Health Information, and Protected Health Information.

"Security Breach" means any actual or potential breach under Applicable Privacy Law with respect to any record or data containing Personal Information or Protected Health Information, and shall include any incident involving the unauthorized access to or acquisition of Personal Information, whether it be encrypted or unencrypted, or in electronic or paper copy, or where the potential exists that encrypted Personal Information or Protected Health Information could be compromised. In the event of any actual or suspected breach involving Protected Health Information, the term Security Breach shall include "breach" as defined in Section 13400 of the HITECH Act (as amended or superseded from time to time), a violation of any provisions under Section 5.12 of this Agreement, the occurrence of a "security incident" as defined in 45 C.F.R. Section 164.304, or any potential or actual security breach or incident as defined by applicable state law.

(a) **Disclosure and Use of Personal Information.** If Service Provider receives, uses, stores, maintains, processes, transmits, disposes or otherwise has access to Personal Information, Service Provider shall use, store, maintain, process, transmit, dispose of and protect Personal Information in accordance with Applicable Privacy Law. Access to and use of Personal Information by Service Provider is specifically limited to that which is necessary to perform the Services set forth in this Agreement and disclosure of Personal Information should be made only to those individuals who have a need to know such information to perform the Services. Service Provider shall obligate its representatives to comply with terms that are at

least as stringent as, and consistent with, those set forth in this paragraph. If Service Provider is required by law to disclose Personal Information, Service Provider shall promptly notify Company in writing (unless prohibited by law) in advance of such disclosure, and provide Company with copies of any unprivileged information to be disclosed to permit Company to take action, if necessary, to object to the release of the Personal Information and Service Provider shall reasonably cooperate with Company in seeking a protective order or other agreement to maintain the confidential nature of the information. At any time that Company requests, if feasible, Service Provider shall securely dispose of all records, electronic or otherwise (including backup records or copies), regarding or including any Personal Information that Service Provider may then possess or control. Disposal may be achieved, at Company's option, through delivery of the records to Company or destruction in a manner that renders the records unreadable and undecipherable by any means. Service Provider agrees to certify in writing to Company that all such Personal Information has been securely destroyed or returned. Further, Service Provider shall comply with Company's Information Security Requirements attached hereto as Exhibit B.

(b) Information Security Program. Service Provider shall develop and implement, within thirty (30) days after the date of execution of this Agreement, if it has not already done so, and thereafter maintain, a comprehensive written information security program that contains administrative, technical, and physical safeguards compliant with Applicable Privacy Law (the "Security Program") designed to: (i) protect the confidentiality, integrity and availability of Personal Information; (ii) protect against anticipated threats or hazards to the security, confidentiality, integrity and/or availability of Personal Information; (iii) protect against any unauthorized access, disclosure or use of Personal Information; (iv) address computer and network security; (v) address physical security; (vi) address business continuity and disaster recovery; (vii) address a security incident response program; and (viii) provide for the secure destruction and disposal of Personal Information. The Security Program shall comply with all Applicable Privacy Law and shall be updated as required by Applicable Privacy Law and industry best practices. Service Provider shall require its contractors who provide services on behalf of Service Provider and who may have access to Personal Information ("Contractors") to develop, implement, and maintain a written Security Program and to provide Service Provider with written acknowledgement of compliance of Contractors' Security Program. Nothing herein should be construed to waive any requirement in any agreement between Service Provider and its Contractors for compliance with Company's security standards and requirements for Personal Information, privacy, data security and network/systems security communicated to Service Provider herein.

(c) Security Breach Reporting. Service Provider shall notify Company within forty-eight (48) hours upon learning of an actual or potential Security Breach involving Personal Information. Service Provider must provide notice to Company's Privacy Office by emailing the Project Manager and must include, at a minimum, and to the extent known, the following information: (a) the nature of the Security Breach; (b) the estimated impact on Company; (c) the name of a senior level person responsible for communicating with Company regarding the Security Breach; and (d) the investigative action taken or planned. Service Provider must reasonably cooperate with the Company's requests for information regarding the Security Breach and Service Provider must provide regular updates on each Security Breach and the investigative and corrective action taken. Any action taken with respect to such Security Breach, including, but not limited to, the investigation and any communication to internal or external parties regarding the Security Breach, will be at the sole discretion of Company unless otherwise required by Applicable Privacy Law.

(d) Indemnity. Service Provider hereby agrees to defend, indemnify, and hold Company and its Affiliates and all of their respective directors, officers, personnel, and their successors and assigns harmless from any and all expenses, damages, awards, settlements, claims, actions and causes of action (in each case regardless of whether sounding in contract, tort, or otherwise), demands, losses, obligations, fines, penalties, liabilities and regulatory actions (including, but not limited to, reasonable attorneys' fees and expenses, breach notification costs, credit monitoring or watch services, internal and external breach remediation plans) arising out of or relating to any privacy or security breach of Personal Information in the possession of or under the control of the Service Provider or its Representatives which is caused by them, or for Service Provider's breach of any obligations set forth in this Section.

5.12 HIPAA and HITECH Privacy and Security Obligations For HIPAA Covered Products

If the Services relate to any HIPAA-covered products, Service Provider shall comply in full with the privacy and security requirements issued pursuant to HIPPA and HITECH as any of the same may be amended or superseded from time to time, including, without limitation, the requirements forth below:

- (a) For the purposes of this Section only, "Individual" means a consumer who is the subject of PHI and seeks to obtain, obtains, or has obtained financial or insurance products or services which are to be used primarily for personal, family, or household purposes.
- (b) Service Provider agrees and acknowledges that it is directly subject to HIPAA (as amended by the HITECH Act and as may be amended or superseded from time to time), including Sections 164.308, 164.310, 164.312 and 164.316 thereof, including its provisions relating to security and privacy of PHI as well as its enforcement and penalty provisions. Service Provider agrees that it shall (i) comply with all applicable security and privacy provisions of HIPAA, as well as all applicable state and local laws and regulations enacted to protect the privacy and security of Individuals' PHI (as any of the same as may be amended or superseded from time to time); and (ii) not act in any way to interfere with or hinder the Company's ability to comply with HIPAA.
- (c) Except to the extent otherwise required or specifically permitted by law, or to the extent specifically provided herein, Service Provider's use and/or disclosure of PHI shall be limited solely to the purposes of performing Services under this Agreement, for the proper management of Service Provider's business to carry out Service Provider's legal responsibilities, or otherwise as required by law.
- (d) In response to an unsolicited direct Individual's inquiry, Service Provider may disclose PHI directly to, and may discuss such information directly with, the Individual to whom such information pertains, provided that such disclosure would not violate HIPAA if Company made it.
- (e) Service Provider may not disclose any PHI to a Nonaffiliated Third Party (as defined under 15 U.S.C. §6809(5) and as amended or superseded from time to time), including but not limited to Service Provider's sub-agents, vendors, contractors, and/or subcontractors, unless such disclosure would be lawful if made directly to the Nonaffiliated Third Party by us. Service Provider agrees and understands that any such disclosure is subject to HITECH, including those provisions related to the sale and marketing of PHI.
- (f) Service Provider shall require that Service Provider's sub-agents, directors, officers, vendors, contractors, Subcontractors and/or employees to whom Service Provider provides, or who otherwise receives PHI to agree in writing to the same restrictions and conditions that apply to Service Provider with respect to such information; provided, however, that Service Provider shall be entitled to provide PHI only to such of its sub-agents, directors, officers and employees who need such PHI to enable them to perform under this Agreement, and then only to the extent necessary for such purpose.
- (g) Service Provider represents and warrants that it and any Subcontractors used in providing the Services shall comply with applicable state and federal privacy and security laws. Service Provider shall enter into written business associate contracts (including the terms required under HIPAA) with each Subcontractor prior to any such Subcontractor having access to Policyholders or any information about Policyholders.
- (h) Service Provider may not use or disclose Protected Health Information in any manner that would constitute a violation of 45 C.F.R. Parts 160 and 164, or 13405(d) of the HITECH Act.
- (i) At the request of and in the time and manner designated by Company, Service Provider shall cooperate with Company in responding to any Individual's (i) request for access to their PHI, and/or (ii) request to amend their PHI.
- (j) Service Provider shall keep a written record of disclosures of PHI that must be provided in an accounting under HIPAA to an individual to whom the PHI relates ("Disclosures"), and shall comply with any request by Company to provide Company with such information regarding such Disclosures, and in such format, as Company reasonably may request.
- (k) In the event that Service Provider receives a request to disclose all or any PHI under the terms of a subpoena or order issued by a court or other governmental body (including without limitation any department of insurance), or any other request for disclosure of PHI, Service Provider agrees: (i) to notify Company of the existence, terms and circumstances surrounding such request within three (3) business days after Service Provider receives the request, and in any event prior to responding thereto, (ii) to comply with any reasonable requests by Company to assist Company in responding to such legal document.
- (l) Service Provider shall limit Service Provider's disclosure of PHI to the minimum necessary for the particular purpose of each disclosure. Service Provider shall only collect such information as is necessary to perform its Services under the Agreement.
- (m) Service Provider represents and warrants that it has implemented and shall maintain administrative, physical and technical safeguards (the "Safeguards") designed to prevent prohibited uses or disclosures, and to protect the confidentiality, integrity and availability, of PHI that Service Provider creates, receives, maintains or transmits. Such safeguards shall include development, implementation, and maintenance of a comprehensive written information security program compliant with Applicable Privacy Law and designed

to (i) protect the integrity and confidentiality of PHI, (ii) protect against anticipated threats or hazards to the security, confidentiality and/or integrity of PHI, (iii) protect against any unauthorized, disclosure, or use of PHI, (iv) address computer and network security, (v) address physical security, and (vi) provide for the secure destruction and disposal of PHI.

(n) In the event Service Provider determines that disclosure of PHI to Service Provider's sub-agents, vendors, contractors, and/or subcontractors is necessary in order to perform under the Agreement or comply with any obligation under this Agreement, Service Provider shall ensure that such sub-agents, vendors, contractors, and/or subcontractors have implemented reasonable and appropriate administrative, physical and technical safeguards to protect PHI.

(o) Service Provider agrees to use its best reasonable efforts to notify Company in writing without delay and in any event within 48 hours upon discovering any Security Breach including (i) a "breach," as the term "breach" is defined in Section 13400, and as the terms "breach" and "discover" are further described in Section 13402(c), of the HITECH Act, (ii) a violation of any provisions under Section 1 of this Agreement, (iii) the occurrence of a "security incident," as defined in 45 C.F.R. Section 164.304, or (iv) a potential or actual security incident as defined by applicable state law. Further, any report of a security incident from Service Provider to Company shall describe the remedial or other action undertaken by Service Provider to correct the current security incident and to prevent future security incidents.

(p) If a security incident or Security Breach occurs, Service Provider shall take reasonable steps to mitigate the adverse impact of the security incident and to prevent future security incidents. Similarly, Service Provider shall mitigate, to the extent practicable, any harmful effect that is known to Service Provider that results from any access, use, disclosure, modification or destruction of PHI in violation of this Agreement.

(q) In the event of an actual or suspected breach or security incident, Service Provider agrees to cooperate fully with Company in any incident investigation or resolution, and agree that no notifications and/or communications to any individual(s), media outlets, state or federal authorities, or other third parties regarding the breach will be made without Company's prior written consent (which consent shall not be unreasonably withheld, conditioned, delayed or denied), unless Applicable Law requires otherwise from Service Provider.

(r) In the event either party learns of a pattern of activity or practice of the other party that constitutes a material breach or violation of its obligations relating to PHI under this Agreement, the non-breaching party will take reasonable steps to cure the breach or end the violation.

(s) If Service Provider has breached Section 5.12 of this Agreement, Company may (i) provide an opportunity for Service Provider to cure the breach within the time specified by Company, or (ii) terminate this Agreement if Company has determined, in its sole discretion, that cure is not possible. If termination is not feasible, Company may report the problem to the Secretary of the U.S. Department of Health and Human Services (the "Secretary"). Notwithstanding the above, Company also reserves the right to terminate this Agreement, at Company's sole discretion, in the event of a material breach or security incident.

(t) Upon termination of this Agreement, if feasible, Service Provider shall return or destroy, in an appropriately secure manner, all PHI without retaining any copies and shall provide Company with Service Provider's written and signed certification to that effect. If such return or destruction is not feasible, Service Provider shall limit all further uses and disclosures to those purposes that make such return or destruction of the PHI not feasible.

(u) Service Provider shall make its internal practices, books and records relating to uses and disclosures of PHI available to Company (or to Company's designee) and to the Secretary, or to the Secretary's designee, for the purpose of confirming Service Provider's compliance and/or Company's compliance with 45 C.F.R. Parts 160 and 164 in connection with the transactions contemplated by this Agreement or as permitted by law.

(v) The parties can mutually agree to amend 5.12 of this Agreement to reflect (i) future amendments of HIPAA, (ii) court orders interpreting the application of HIPAA, or (iii) a material change in Company's business practices.

(w) At the request of and in the time and manner designated by Company or its Affiliates, Service Provider shall provide access to PHI then in its control or possession or in the possession or control of its Subcontractors or vendors to Company or its Affiliates, or, as directed by Company or its Affiliates, to a Policyholder. If a Policyholder contacts Service Provider directly about access to his or her PHI, Service Provider shall not provide such access, but rather shall forward such request to Company and its Affiliates

in writing within five (5) days after having received the request. Notwithstanding the above, Service Provider shall cooperate with Company and its Affiliates in responding to any such request.

(x) At the request of and in the time and manner designated by Company and its Affiliates, Service Provider shall amend PHI in its possession or control or in the possession or control of its vendors and/or Subcontractors. If a Policyholder contacts Service Provider directly about amending his or her PHI, Service Provider shall not make such amendment but rather shall forward such request to Company and its Affiliates within five (5) business days after having received the request. Notwithstanding the above, Service Provider shall cooperate with Company and its Affiliates in responding to any such request.

(y) Service Provider shall comply with such other restrictions on the use or disclosure of Protected Health Information as required under 45 C.F.R. §164.504(e), as may be amended from time to time or as may be required under any controlling judicial, quasi-judicial or administrative decision, ruling, opinion, policy or other authority with respect to 45 C.F.R. §164.504(e).

(z) The provisions of Section 5.12 of this Agreement shall survive the termination of this Agreement and/or the return or destruction of PHI.

(aa) Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits compliance with HIPAA.

(bb) Service Provider obligations with respect to Protected Health Information shall survive the termination of this Agreement and/or the return or destruction of any Protected Health Information and shall survive until the fifth (5th) anniversary of termination of this Agreement or the sixth (6th) anniversary of the last date on which Services are provided by Service Provider, whichever is later.

5.13 Compliance with GLBA. Service Provider shall comply with the privacy requirements of the GLBA and the rules and regulations promulgated thereunder (as any of the same may be amended or superseded from time to time, "GLBA"), as set forth below:

- (a) Except to the extent otherwise required or specifically permitted by law, or to the extent specifically provided herein, Service Provider use and/or disclosure of Policyholder Confidential Information shall be limited solely to the purposes for which it is disclosed to Service Provider to perform its obligations under this Agreement.
- (b) Service Provider shall require that its agents, directors, officers, and employees to whom it provides, or who otherwise receive Policyholder Confidential Information to agree to substantially the same restrictions and conditions that apply to Service Provider with respect to such information.
- (c) Service Provider shall implement appropriate measures to ensure the security and confidentiality of Policyholder Confidential Information.

6. WARRANTIES

6.1 Deliverables. Service Provider represents and warrants that all Deliverables, when accepted, will meet the applicable Specifications set forth in the applicable Statement of Work. Any tools used in conjunction with the Deliverables will be tested for value, security, and appropriateness to the task prior to being used. Unless otherwise set forth in a SOW, within ninety (90) days from the date of Company's receipt of the Deliverables, Service Provider warrants that it will correct, without charge to Company, any Deliverables that fail to conform in accordance with the applicable Statement of Work.

6.2 Services. Service Provider represents and warrants that all Services will be performed in a competent, professional and workmanlike manner and in conformity with the requirements set forth in each applicable Statement of Work or in any exhibits or schedules attached thereto and consistent, competent, professional manner and in accordance with the terms of this Agreement, Applicable Law, and industry standards. Unless otherwise set forth in a SOW, within ninety (90) days from the date of Company's receipt of the Services, Service Provider warrants that it will correct, without charge to Company, any Services that fail to conform to the applicable Statement of Work.

6.3 Sufficient Resources. Service Provider represents and warrants that it shall provide sufficient employees and facilities to perform its obligations under this Agreement to perform the Services within the applicable time frames agreed to by the parties and that such employees have sufficient skill, knowledge and training to perform the Services.

6.4 **Intellectual Property Assignments.** Service Provider represents and warrants that: (i) all Employees and Representatives utilized by Service Provider in performing Services for Company are under a written obligation to Service Provider requiring such persons to maintain the Proprietary Information of Service Provider's customers and (ii) with respect to Employees, to assign all of such person's right, title and interest to Service Provider in and to any Services and Deliverables which are developed, prepared, conceived, made or suggested by such person while providing Services on behalf of Service Provider. In addition, prior to commencement of any work under this Agreement, Service Provider shall require all Employees and Representatives utilized by Service Provider to individually sign a confidentiality and nondisclosure agreement with provisions as least as restrictive as those set forth in this Agreement.

6.5 **Actions, Suits or Proceedings.** Service Provider represents and warrants that there are no actions, suits, proceedings or investigations, pending or, to the best of its knowledge, threatened, that could have a material adverse effect on Service Provider's ability to fulfill its obligations under this Agreement. Service Provider further warrants that it shall immediately notify Company if, during the term of this Agreement, Service Provider becomes aware of any action, suit or proceeding, pending or threatened, that could have a material adverse effect on Service Provider's ability to fulfill its obligations under this Agreement.

6.6 **Non-Infringement.** Each party represents and warrants to the other party that any goods, services or information provided to the other party for its use pursuant to this Agreement, and Service Provider represents and warrants that the creation of any work product, including, without limitation, any of the Services or Deliverables, do not and shall not infringe any third party patent, copyright, Trade Secret, trademark or other Intellectual Property rights of any kind without limitation, and there is no actual or threatened claim or lawsuit by any third party for infringement of such rights. Each party further represents and warrants that it shall promptly inform the other party if, after the Effective Date of this Agreement, such party receives an actual or threatened claim or lawsuit by any third party based on a violation of such rights.

6.7 **Compliance with Applicable Law.** Service Provider represents and warrants that the Services and Deliverables being provided by Service Provider, as well as its employees, agents, representatives, affiliates and Subcontractors shall at all times comply with all Applicable Law. Service Provider further represents and warrants that it will have obtained any necessary permits, licenses, certificates or any other documentation and authorization required to comply with any such laws and regulations or for Service Provider to perform the Services and/or its other obligations under this Agreement. Company and its Affiliates represent and warrant that they will comply with all applicable laws, rules and regulations, and not use or disclose any of the Deliverables for any purpose not authorized in this Agreement.

6.8 **Virus Protection.** If any software is provided to Company as part of the Services or Deliverables, Service Provider represents and warrants that it shall use the most effective methods and techniques reasonably available to Service Provider to check the software, prior to delivery to Company, for the presence of Viruses and to remove and destroy any such Viruses found in the software and, to the best of Service Provider's knowledge at the time of submission, the software delivered hereunder contains no Viruses. If the installation of the software by Company transfers to Company's computers a Virus, Service Provider shall reimburse Company the reasonable cost incurred by Company including costs of persons employed by Company to remove and recover from such Virus.

6.9 **Absence of Disabling Devices.** If any software is provided to Company as part of the Services or Deliverables, Service Provider represents and warrants that none of the software contains, or will contain, any Self-Help Code or any undisclosed Unauthorized Code or similar malicious computer instructions, intentional devices or techniques that can or were designed to threaten, infect, attach, assault, vandalize, defraud, disrupt, damage, disable, improperly access, interfere with, cause damage to, or shut down a computer system or any component of such computer system, including its security or user data.

6.10 **Functionality of Programming.** Any software developed or delivered as part of the Deliverables shall conform to and perform in the computer environment agreed to by Service Provider and Company. This warranty may be immediately terminated if any modification is made to the source code by non-Service Provider personnel without Service Provider's consent or direction. Service Provider will charge Company for costs incurred and time spent, as set forth in Section 4, if the cause of error was not within the software as delivered or required to be delivered to Company. Service Provider further warrants that all Deliverables shall correctly function without additional modification, additional

programming, or manual intervention with regard to any use, handling, storage, processing, calculation, reference, or transference of information and/or data for any period of time after 1999. Service Provider warrants that the functionality of all Deliverables shall not be impaired, altered, or changed with respect to the use of data or records containing dates falling prior to, on or after January 1, 2000.

7. REMEDIES AND LIMITATIONS

7.1 Material Breach. In the event that either party commits a material breach of any provision of this Agreement, including, without limitation, any of the warranties set forth in Section 6 above, the other party is, unless otherwise provided for herein, entitled to avail itself of any and all legal and equitable remedies, including the right to terminate as set forth in Section 9.

7.2 Nonconformity of Services. In the event Company notifies Service Provider of any nonconformity with respect to the warranties set forth in Section 6, Service Provider shall, at its own expense, promptly re-perform the Service or correct such nonconformity as necessary to bring the Deliverable into conformity with the applicable Specifications. Service Provider's curative efforts are to be completed within fifteen (15) business days (the "Cure Period"), unless a different period is set forth in an applicable Statement of Work. In the event Service Provider is unable to cure such nonconformity within the Cure Period, Company may immediately terminate the applicable Statement of Work.

7.3 Dispute Resolution.

(a) **Negotiation.** Except where injunctive relief is sought, each party shall attempt in good faith to resolve any controversy, claim or dispute of whatever nature arising out of or relating to this Agreement or the breach, termination, enforceability or validity thereof ("Dispute") promptly by negotiation between executives or managers who have authority to settle the Dispute and who are at a higher level of management within each of the parties' organizations than the parties' appointed Project Managers. Each party shall provide the other with all unprivileged information and documentation relied upon by the party to substantiate its position with respect to the Dispute other than attorney work product.

(b) **Waiver of Right to Jury Trial.** If the parties are unable to resolve a Dispute using the mechanisms described above, then either party is entitled to any and all legal and equitable remedies available. However, Company and Service Provider agree not to seek, and each hereby waives any right to, trial by jury in any action, proceeding or counterclaim brought by either of them against the other on any matter or claim arising out of or in any way relating to this Agreement, a Statement of Work, the relationship of Company and Service Provider, the performance or non-performance of the Services, any claim of injury or damage, or the enforcement of any remedy under any law, irrespective of whether any such matter or claim is based in contract, in tort or otherwise. Neither party shall seek to consolidate any such action in which the right to trial by jury has been waived with any other action in which such right has not been or cannot be waived, it being the intention of the parties that the jury trial waiver be subject to no exceptions.

7.4 Other Remedies. Each party agrees and acknowledges that breach of this Agreement may cause the other irreparable harm without an adequate remedy at law and hereby agrees that the other party may seek temporary or permanent injunctive relief to prevent or limit the effect of any such breach.

7.5 Attorney Fees. If any dispute arises between the parties hereto concerning the breach, enforcement or interpretation of any provision of this Agreement, then the prevailing party shall be reimbursed its court costs, reasonable attorneys' and expert witness fees and disbursements, and all other costs and expenses incurred by the other party on account thereof, including those incurred in connection with any matters on appeal.

7.6 Limitation of Liability.

EXCEPT AS OTHERWISE STATED HEREIN OR FOR FRAUD, MALICIOUS, WILLFUL OR INTENTIONAL TORTIOUS ACTS; BREACHES OF CONFIDENTIALITY; OBLIGATIONS TO INDEMNIFY AND CLAIMS ARISING OUT OF OR RELATING TO PROPERTY DAMAGE, PERSONAL INJURY AND/OR DEATH, NEITHER PARTY'S TOTAL LIABILITY TO THE OTHER ARISING OUT OF OR RELATING TO THIS AGREEMENT, WHETHER BASED ON CONTRACT, TORT OR ANY OTHER LEGAL THEORY, SHALL NOT EXCEED FOUR TIMES THE AMOUNT OF FEES PAID AND TO BE PAID BY COMPANY AND ITS

AFFILIATES TO SERVICE PROVIDER DURING THE TERM OF THIS AGREEMENT. EXCEPT WITH RESPECT TO OBLIGATIONS TO INDEMNIFY, NEITHER PARTY BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, EXEMPLARY, PUNITIVE, SPECIAL OR SIMILAR DAMAGES INCLUDING, WITHOUT LIMITATION, LOSS OF PROFITS OR LOSS OF REVENUES, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE LIKELIHOOD OF THE OCCURRENCE OF SUCH DAMAGES OR SUCH DAMAGES ARE FORESEEABLE.

8. INDEMNITY

8.1 **Indemnification for Service Provider Acts and Omissions.** Service Provider, its Affiliates and successors in interest, shall and hereby does indemnify, defend and hold harmless Company and its Affiliates, and their respective shareholders, Representatives, successors and assigns harmless from and against any and all expenses, costs damages, claims, actions and causes of action (in each case whether sounding in contract, tort or otherwise), demands, losses, obligations, fines, penalties and liabilities (including, but not limited to, reasonable attorneys' fees and expenses) resulting in any manner from the performance or non-performance of Service Provider or its Affiliates, or any of their respective shareholders and Representatives (collectively, the "Service Provider Parties") arising out of (i) any breach by Service Provider Parties or those acting for or on behalf of Service Provider of any of Service Provider's obligations hereunder; (ii) any negligent or wrongful act or omission on the part of any of the Service Provider Parties in the performance or nonperformance of any duty or obligation required to be performed by Service Provider under this Agreement; (iii) fraud, bad faith, illegal act or omission, negligence (including professional negligence) or willful misconduct by Service Provider or its Representatives or any other person acting at the direction or under the control of Service Provider; (iv) any breach by any of the Service Provider Parties of the representations, warranties, duties and/or obligations of Service Provider under this Agreement; and (v) any act by Service Provider that is beyond the scope of its authority hereunder; provided that, any acts or omissions by Service Provider or its Representatives causing damage will not require indemnification to the extent arising from the willful or negligent acts of Company, its employees or agents.

8.2 **Indemnification for Company Acts and Omissions.** Company agrees to defend, indemnify and hold Service Provider and its shareholders, Representatives, successors and assigns harmless from any and all expenses, damages, claims, actions, demands, losses, liabilities and causes of action (including, but not limited to, attorneys' fees and expenses) to the extent arising out of or relating to a breach of this Agreement or Applicable Law, or the willful or negligent acts or omissions on the part of Company, its employees or agents, including, but not limited to, injury or death to all persons as well as damage to any real or personal property.

8.3 **Personnel.** Service Provider agrees to defend, indemnify and hold Company and its Affiliates and all of their shareholders, Representatives, successors and assigns harmless from and against any and all expenses, damages, claims, actions, demands, losses, fines, penalties, liabilities and causes of action (including, but not limited to, reasonable attorneys' fees and expenses) arising out of or relating to withholding taxes, unemployment or workers compensation, employee benefits or compensation, employment claims, or any other claim, demand, liability or loss of any nature relating to the personnel supplied to Company or providing Services to Company under this Agreement.

8.4 **Indemnification for Intellectual Property Infringement.**

(a) **Obligation to Indemnify.** Service Provider agrees to defend, indemnify and hold Company and its Affiliates and all of their shareholders, Representatives, successors and assigns harmless from and against any and all expenses, damages, claims, actions and causes of action (whether sounding in contract, tort or otherwise), demands, losses and liabilities (including, but not limited to, reasonable attorneys' fees and expenses) arising out of or relating to infringement or alleged infringement of any patent, copyright, Trade Secret, trademark or other Intellectual Property rights for or on account of the manufacture, distribution, sale or use of any results, Services or Deliverables furnished hereunder. Service Provider is not required to indemnify where (i) such matter arises due to Company's actions or omissions contrary to the documentation applicable to the Deliverables from which the infringement is claimed, or (ii) compliance by Service Provider with detailed specifications prescribed by or originating with Company that constitutes the basis of the infringement or alleged infringement.

(b) **Application to Software.** This Section 8.4 applies to any software licensed or used by Company as part of the Services described in any Statement of Work, including, without limitation, a pilot project or proof

of concept, until such time as any such software becomes the subject of a separate licensing agreement between Service Provider and Company that by its terms expressly supersedes the indemnification obligations in this Section.

8.5 **Conditions Precedent.** For any indemnification claim under Section 8, the party seeking indemnity shall promptly notify the other party in writing of any claim, demand, suit or proceeding, together with any and all documentation related to such claim, demand, suit or proceeding. The indemnifying party shall have full authority to control the defense of such suit at its expense; however no admission of liability on behalf of the indemnified party will be made without prior written consent from the indemnified party. The indemnifying party may not settle any claim unless the claimant gives a full unconditional release of all liability. The party seeking indemnification may participate at its own expense. The failure of a party seeking indemnity under this Section to provide the other party with prompt notice does not relieve the party providing indemnification of its obligations under this Section 8, unless such failure to promptly notify the party providing indemnity causes such party material prejudice. No settlement that prevents Company from continuing to use the results, Services and Deliverables shall be made without Company's prior written consent, which consent shall not be unreasonably withheld, conditioned, delayed or denied.

9. **TERM AND TERMINATION**

9.1 **Term of Agreement.** This Agreement is to commence as of the Effective Date of this Agreement and is effective until terminated as provided herein ("Term"). Each Statement of Work issued hereunder becomes effective as of the effective date specified in the Statement of Work and continues for the Term specified in the Statement of Work, unless terminated earlier as provided herein. Company Affiliates may enter into Statements of Work with Service Provider under the terms of this Agreement. The references to Company for purposes of this Section, applies to any Company Affiliate which has entered into a separate Statement of Work with Service Provider, except that a Company Affiliate alone shall not have the authority to terminate this Agreement as to Company or any other Company Affiliates, and the Company Affiliate, and not Company, is the responsible party for the Statement of Work. Notwithstanding anything in this Agreement to the contrary, Company shall have the option of terminating one or more Statements of Work without terminating this Agreement or any other Statements of Work.

9.2 **Termination for Convenience.**

(a) **Termination of Agreement.** Company or Service Provider may in its sole discretion terminate this Agreement without cause and for convenience by giving the other party at least ninety (90) business days' prior written notice of the termination; provided, however, that this Agreement shall continue to remain in effect with respect to any Statement of Work(s) outstanding as of the date of such termination, until such Statement of Work(s) are themselves either completed or terminated.

(b) **Suspension or Termination of Statement of Work.** A Statement of Work may, if expressly so indicated, provide for its own term and termination, but such termination in and of itself will not terminate this Agreement. Any Statement of Work may be suspended or terminated in whole or in part upon written notice from Company, with or without cause. Upon receipt of notice of suspension or termination, Service Provider shall inform Company of the extent to which performance has been completed through such date, and collect and deliver to Company (or otherwise as Company may reasonably request) whatever Deliverables then exist in a manner reasonably prescribed by Company in accordance with this Agreement. Service Provider shall be paid for all Deliverables of Service Provider that conform to the Specifications or otherwise meet this Agreement's requirements through the date of suspension or termination, provided that such payment shall not be greater than the payment that would have become due if the work had been completed. Service Provider may not suspend or terminate any Statement of Work once Service Provider has begun performance of the Services.

9.3 **Termination for Cause.**

(a) **Material Default.** If either party materially defaults in the performance of any of its obligations under this Agreement or any Statement of Work, the non-defaulting party may immediately terminate this Agreement and all outstanding Statements of Work as of a date specified in such notice of termination. For purposes hereof, a party shall be deemed to be in material default if it: (a) materially breaches any of its duties, obligations or responsibilities under this Agreement or a Statement of Work which default is not

10. **INSURANCE**

10.1 **Coverage Amounts.** Without limiting Service Provider's undertaking to defend, indemnify and hold Company harmless as set forth herein, Service Provider shall obtain and maintain insurance with the following coverages and terms:

- (a) Commercial General Liability coverage, including contractual liability for all written contracts, personal injury liability and completed operations coverage with \$2,000,000 combined single limit of liability for each occurrence and in the aggregate for bodily injury and property damage.
- (b) Professional or Errors and Omissions Insurance providing liability coverage for the professional services to be performed under this Agreement with \$10,000,000 limits of liability for any one claim made.
- (c) Workers compensation insurance with statutory limits covering Service Provider's workforce, affording protection in any state in which Service Provider's workforce may operate, including Employer's liability insurance with \$1,000,000 limits of liability; alternate employers endorsement to workers compensation policy.
- (d) Business automobile liability covering all owned, non-owned hired autos and autos owned or borrowed by workers or contractors while used in the course of their employment with \$1,000,000 limits of liability for bodily injury and property damage arising out of any one accident.
- (e) Excess or Umbrella Liability coverage with a minimum limit of four million dollars (\$4,000,000) coverage in excess of the coverage as set forth in items 10.1 above
- (f) Commercial Blanket Employee Fidelity Insurance providing \$1,000,000 limits of primary coverage for all Service Provider's workers and all of its contractors or subcontractors of every tier, including legal liability coverage for loss of Company's money, securities or property through fraudulent or dishonest acts.

10.2 **Insurance Company Ratings.** Service Provider shall provide insurance coverage by insurance companies having policy holder ratings no lower than "-A" and financial ratings not lower than "VII" in the latest edition of Best's Insurance Guide in effect as of the date of this Agreement.

10.3 **Certificates of Insurance.**

- (a) **Provide to Company.** Service Provider shall immediately submit and, upon renewal of such insurance coverage, certificates of insurance to Company as evidence that the specified forms, endorsements and amounts of insurance as required are in force. All certificates shall include a clause obligating the insurer(s) to give the certificate holder not less than thirty (30) days prior written notice of any material change in, cancellation of, or intent not to renew the insurance.
- (b) **Requirements for Subcontractors.** Service Provider shall require similar insurance and maintain on file certificates of insurance from its Subcontractors of every tier, providing copies of certificates to Company upon reasonable request.

10.4 **No Restriction.** The insurance policies listed above are restricted by the country or state in which any Services are being performed. In the case of Services performed outside the United States where insurance is required by law, the insurance must be placed with a company admitted to do business in that country.

10.5 **Primary Coverage.** The foregoing insurance coverage is primary and non-contributing with respect to any other insurance or self-insurance that may be maintained by Company and its Affiliates and shall contain a cross-liability or severability-of-interest clause.

10.6 **Inclusion of Company and its Affiliates.** Company and its Affiliates shall be specifically included as an additional insured under the following coverage, if required: commercial general liability, commercial automobile/trucker's coverage/motor carrier coverage, and umbrella/excess liability coverage, for liability or loss arising out of or in any way associated with any act, error, omission or product of Service Provider, its directors, officers, shareholders, its workforce or anyone else for whose acts or products Service Provider may be held responsible (with coverage to Company at least as broad as that which is provided to Service Provider and not lessened or avoided by endorsement).

10.7 **Deductibles.** All deductibles or self-insured retentions are the sole responsibility of Service Provider.

10.8 **Term for Insurance.** All liability insurance requirements shall remain in effect for 2 years after termination of this Agreement.

10.9 **Service Provider's Separate Insurance Obligations.** The insurance obligations imposed by this Section are separate and distinct from any indemnification obligations imposed by this Agreement. Service Provider agrees that carrying insurance as required in this Agreement shall in no manner lessens nor affects Service Provider's other obligations or liabilities set forth in this Agreement, including without limitation any indemnification obligation.

11. **GENERAL**

11.1 **Assignment.** Each party agrees it will not to assign this Agreement without the other party's prior written consent (which consent shall not be unreasonably withheld), and that any attempt to do so is void and has no effect. All such assignments (except to the extent that this Agreement expressly provides otherwise) are prohibited.

11.2 **Binding Effect.** This Agreement will be binding upon and inure to the benefit of the parties hereto and their respective successors and permitted assigns.

11.3 **Governing Law.** The substantive and procedural laws of the State of Delaware (without giving effect to its conflicts of law principles and without regard to the Uniform Computer Information Transactions Act ("UCITA") or any version or revision of UCITA govern all matters arising out of or relating to this Agreement or any Statement of Work, including, without limitation, its validity, interpretation, construction, performance and enforcement. The provisions of the United Nations Convention on Contracts for the International Sale of Goods do not apply to this Agreement or to any Statement of Work.

11.4 **Venue.** The parties consent to the exclusive jurisdiction of, and venue in, any federal or state court of competent jurisdiction located in Federal Court in Delaware for the purposes of adjudicating any matter arising out of or relating to this Agreement or any Statement of Work.

11.5 **Notices.** All notices required to be given to a party under this Agreement are to be delivered to the following addresses, or any other addresses designated by the parties by notices delivered in accordance with this Section:

If to Service Provider: Examination Management Services, Inc.
3050 Regent Boulevard, Suite 400
Irving, Texas 75063
Attn: General Counsel

If to Company: Transamerica Procurement MS: 1130
4333 Edgewood Rd NE
Cedar Rapids, IA 52499

With a separately delivered copy to:
General Counsel
Money Services, Inc.
4333 Edgewood Rd NE
Cedar Rapids, Iowa 52499

Any notice required or permitted under this Agreement is to be given in writing and is deemed effectively given: (a) upon personal delivery to the party to be notified; (b) upon confirmation of receipt by fax by the party to be notified; or (c) deposit with a reputable overnight courier, prepaid for overnight delivery and addressed as set forth in this Section and upon confirmation of delivery to recipient.

11.6 **No Waiver.** The failure of a party to enforce any provision, exercise a right or pursue a default of this Agreement shall not be considered a waiver of its rights. The express waiver of a provision will be effective only in the specific instance, and as to the specific purpose, for which it was given. Unless stated otherwise, all remedies

provided for in this Agreement are to be cumulative and in addition to, and not in lieu of, any other remedies available to either party at law, in equity or otherwise.

11.7 **Severability.** Any part or provision of this Agreement that is held to be inoperative, unenforceable, voidable or invalid in any jurisdiction shall, as to that jurisdiction, be inoperable, unenforceable, void or invalid without affecting the remaining provisions in that jurisdiction or the operation, enforceability, or validity of that part or provision or any other provision in any other jurisdiction, and to this end, the provisions of this Agreement are declared to be severable. Should any part or provision of this Agreement be held inoperative, unenforceable, voidable or invalid in any jurisdiction, such part or provision shall, as to that jurisdiction, be replaced with a provision that accomplishes, to the extent possible and lawful, the original business purpose and economic intent of such part or provision in a valid and enforceable manner, and the remainder of this Agreement shall remain effective and binding upon the parties hereto. In the event the ruling and/or the controlling principle of law or equity leading to the holding is subsequently overruled, modified, or amended by legislative, judicial, or administrative action, the part or provision(s) in question as originally set forth in this Agreement shall be deemed valid and enforceable to the maximum extent permitted by the new controlling principle of law or equity.

11.8 **Effect of Headings.** The section headings contained in this Agreement are for convenience only and do not affect the construction or interpretation of any provision of this Agreement.

11.9 **Authorship/Fees and Expenses.** This Agreement is the result of arm's length negotiations between the parties and each of the parties has agreed to the use of the particular language in this Agreement. The parties further acknowledge that any questions of doubtful or unclear interpretation are not to be resolved by any rule or interpretation against the drafters, and that each party has participated in drafting this Agreement. Accordingly, this Agreement is to be construed without regard to the party or parties responsible for its drafting or preparation. Except as expressly provided in this Agreement, each party hereto shall be responsible for all fees, costs and expenses incurred by that party in connection with the preparation of and performance under this Agreement.

11.10 **Force Majeure.** Neither party is to be liable to the other party for any failure or delay caused by Force Majeure. The date of performance for the nonperforming party shall be extended for a period equal to the time lost by reason of any delay arising directly from any Force Majeure event, provided however that if the Force Majeure event lasts more than thirty (30) business days, Company has the right to immediately terminate this Agreement with no further obligations to Service Provider.

11.11 **Counterparts.** This Agreement may be executed in counterparts and delivered to each of the parties by facsimile. Facsimile or PDF signatures are deemed as legally enforceable as the original. Each such counterpart is deemed an original instrument, but all such counterparts taken together constitute one and the same agreement.

11.12 **Survival.** Upon termination of this Agreement for any reason, any section that by its nature should survive this Agreement to be effective shall survive and continue in full force and effect and be binding upon the parties, including, without limitation, Sections 4, 5, 6, 7, 8, 9.4, 9.5, 10 and 11.

11.13 **Business Forms Terms and Conditions.** If the terms and conditions in any purchase order or sales order, invoice, quote form or any other business form conflict with this Agreement, the terms and conditions contained in this Agreement are controlling.

11.14. **No Solicitation.** Each party agrees that during the term of this Agreement and for a period of one (1) year after the termination of this Agreement, it will not, except as part of an advertisement of employment opportunities in a publication of general circulation: (i) hire any person who is at any time during the term of this Agreement an employee of the other party or an Affiliate of the other party; (ii) directly solicit, entice, induce or encourage any person who is at any time during the term of this Agreement an employee of the other party or an Affiliate of the other party; or (iii) directly approach any such employee of the other party or an Affiliate of the other party for such purpose or authorize or knowingly approve the taking of such actions by any other person, corporation or entity, in each case without the express written consent of the employee's employer, which consent may be withheld in the sole and absolute discretion of the employer. The provisions of this Section shall survive termination of this Agreement as necessary to affect its purpose. Notwithstanding the foregoing, the above limitation does not apply in

the event an employee of either party or of an Affiliate has independently submitted his or her resume to an employment agency or recruiter, and such employment agency or recruiter forwards such resume or other information on to either party.

11.15. **Examination Rights.** Company shall have the right upon not less than fifteen (15) business days prior written notice, to examine and copy applicable records and practices of the Service Provider for the purpose of confirming compliance with the terms of this Agreement and of any Statement of Work. Such right shall be exercised no more than once annually during normal business hours and in a manner that does not unreasonably interfere with the business operations of the Service Provider. If the examination discloses an overpayment of any amount due by Company under this Agreement by more than ten percent (10%), Service Provider shall reimburse Company's reasonable expenses of examination.

11.16 **Regulatory Compliance and Assurances**

- (a) During the Term of this Agreement, Service Provider shall perform its obligations herein in such a manner as to be in full compliance with all applicable Federal and state regulations. Service Provider shall provide Company with all data and reports necessary for Company to comply with all Federal and state regulations applicable to the Services provided by Service Provider.
- (b) Provided that such enactments or regulations do not prohibit Service Provider from performing the Services for Company, Service Provider shall use commercially reasonable efforts to perform the Services regardless of changes in legislative enactments or regulatory requirements. If such changes prevent Service Provider from performing its obligations under this Agreement, Service Provider shall, when appropriate, make commercially reasonable efforts to develop and implement a suitable temporary work around until such time as Service Provider can perform its obligations under this Agreement without such temporary work around.
- (c) Service Provider and Company acknowledge and agree that the performance of the Services will be subject to regulation and examination by Company's regulatory agencies to the same extent as if such Services were being performed by Company. Upon reasonable request, Service Provider agrees to provide any appropriate assurances to such agency and agrees to subject itself to any appropriate examination or regulation.

11.17 **Foreign Corrupt Practices Act.** Service Provider shall not violate, or cause Company to violate the United States Foreign Corrupt Practices Act or any other similar applicable anticorruption laws or regulations ("FCPA") in connection with the Services and has not, and agrees that it shall not, in connection with the transactions contemplated by the Agreement, or in connection with any other business transactions involving Company or any Company Affiliate pay, offer, promise, or authorize the payment or transfer of anything of value, directly or indirectly to any government official or employee (including employees of government owned or controlled companies or public international organizations) or to any political party, party official, or candidate for public office, or any other person or entity, if such payments or transfers would violate the laws of the country in which made or the laws of the United States.

It is the intent of the parties that no payments or transfers of value by Company or Service Provider in connection with this Agreement shall be made which have the purpose or effect of public or commercial bribery, or acceptance of or acquiescence in, extortion, kickbacks, or other unlawful or improper means of obtaining business.

11.18 **Entire Agreement.** This Agreement, including all Statements of Work, schedules, amendments, appendices and other attachments, constitutes the complete and exclusive statement of the agreement between Service Provider and Company and supersedes all prior oral or written proposals, prior agreements and other prior communications between the parties, concerning the subject matter of this Agreement, except for prior provisions regarding confidentiality and nondisclosure. No amendment, waiver or modification of this Agreement is binding unless it is in a writing that explicitly references this Agreement and is signed by authorized representatives of both parties.

IN WITNESS WHEREOF, the parties have entered into this Agreement as of the Effective Date. Each signatory to this Agreement represents and warrants that he or she possesses all necessary capacity and authority to duly execute and deliver this Agreement on behalf of the entity for which such person is signing.

Company

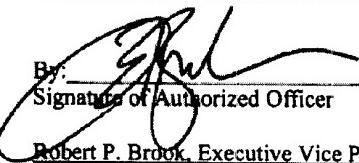
MONEY SERVICES, INC.

By: 
Signature of Authorized Officer

Bob Plaza, Vice President
Printed Name and Title

Service Provider

EXAMINATION MANAGEMENT SERVICES, INC.

By: 
Signature of Authorized Officer

Robert P. Brook, Executive Vice President and CDO
Printed Name and Title

EXHIBIT A

TEMPLATE

MONEY SERVICES, INC.

STATEMENT OF WORK

IN WITNESS WHEREOF, the parties have entered into this Statement of Work as of the date written above.

Company

MONEY SERVICES, INC.

By:

Signature of Authorized Officer

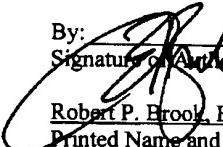
Printed Name and Title

Service Provider

EXAMINATION MANAGEMENT SERVICES, INC.

By:

Signature of Authorized Officer

 Robert P. Brook, Executive Vice President & CDO

Printed Name and Title

**INFORMATION SECURITY
EXHIBIT B**

1. **Overview.** The purpose of this Attachment is to define the Information Security practices that Service Provider is required to establish, administer and maintain to protect Company Information Assets.
2. **Policy.** It is Company's policy that the following Information Security practices be established, administered and maintained by any third party having access to Company Information Assets, without exception.
3. **Definitions for purposes of the Information Security Requirements Exhibit B.**
 - a. "Agent" means anyone who, through either an agency or contractual relationship, has authority to view, host, store, process, transmit, print, back-up or destroy Company Information Assets.
 - b. "Agreement" means the contract entered into between the Company and the Service Provider, and to which this document is attached as an Attachment.
 - c. "Company Information Assets" are Information Assets belonging to or under the control of Company, including without limitation, all information and data provided by Company to Service Provider in any form, and any information or data generated as a result thereof (excluding any information that is properly of public record or that Company provides written permission for its disclosure).
 - d. "Information Assets" are defined as information and data in any form, whether electronic, hardcopy, photographic image, microfiche or microfilm or in digital, magnetic, optical or electronic form. It also includes all computing, network, and telecommunications systems and equipment which view, host, store, process, transmit, print, back-up or destroy information and data (e.g. personal computers, laptops, workstations, servers, network devices, software, portable storage devices, electronic storage media, cabling, and other computing and infrastructure equipment).
 - e. "Information Security" is defined as the protection against the loss of Information Assets' confidentiality, integrity and availability.
 - f. "Information Security Breach" is defined as any unauthorized act that bypasses or contravenes Company's information security measures as defined herein. It also encompasses the unauthorized use or disclosure of, or unauthorized access to or acquisition of, Company Information Assets.
 - g. "Information Security Program" is defined as the collection of policies, standards, procedures and controls, taken as a whole and implemented by Company or Service Provider, that are designed to protect the confidentiality, integrity, and availability of Information Assets.
 - h. "Information Security Vulnerability" is defined as a weakness in information security controls which could be exploited to gain unauthorized access to Company Information Assets.
 - i. "Physical Security" or "Physically Secured" is defined as the protection of information in hardcopy form against loss or unauthorized acquisition, access or disclosure during its production, storage, distribution, use or destruction. It also encompasses the protection of information technology hardware, infrastructure and facilities, as well as power or environmental control utilities used in data processing operations to protect against damage, destruction, or misuse of Information Assets.
4. **Organizational Roles and Responsibilities.** Service Provider organizational roles and responsibilities must include a chief information security officer, or comparable role assigned to one of Service Provider's officers or

senior management, to be responsible for the establishment, administration, and maintenance of a comprehensive written Information Security Program. The Information Security Program must include, at a minimum, the practices described in this Attachment.

5. **Non-Disclosure of Company Information Assets.** Service Provider acknowledges that the unauthorized release or misuse of the Information Assets could cause harm to the business reputation of either or both Service Provider and Company. Service Provider will not, and will cause its employees and Agents engaged in providing services to Company to not, knowingly take any action or omission which would result in the unauthorized release or misuse of the Information Assets of Company. Any actual or suspected Information Security Breach experienced by Service Provider involving Company Information Assets, must be reported by Service Provider to Company within forty-eight (48) hours of its detection.
6. **Information Security Framework and Right to Audit.**
 - a. The Service Provider's Information Security Program shall conform to the framework set forth by the International Standards Organization in a standards document entitled "Code of practice for information security management" (ISO/IEC 27002:2005, and as may be amended from time to time.). In addition to the standards outlined therein, Service Provider's Information Security Program must include the practices described in this Attachment. Service Provider's Information Security Program must be reviewed annually or whenever there is a material change in business practices that may implicate the security posture.
 - b. At Company's expense, promptly upon receipt of Company's written request, Service Provider shall grant Company, or a third party on Company's behalf, permission to perform an audit or assessment of Service Provider's compliance with the Information Security Program requirements at least annually. Following any Information Security Breach of Service Provider involving Company Information Assets such audit will be done at Service Provider's expense. The audits or assessments may be written or physical or as otherwise determined by Company. At Company's request at any time during the term of this Agreement, Service Provider agrees to certify in writing to Company Service Provider's compliance with the terms of this Attachment.
 - c. Service Provider, promptly upon receipt of Company's written request shall (a) provide to Company a report expressing the opinion of an independent third-party who, at the time of the review, holds current certifications as both a Certified Information Systems Auditor (CISA) from the Information Systems Audit and Control Association (ISACA) and a Certified Information Systems Security Professional (CISSP) from the International Information Systems Security Certification Consortium ("(ISC)2") on the effectiveness of Service Provider's information security controls; or (b) respond to any reasonable Company requests for information regarding Service Provider's information security program and practices. This request can be no more than annually unless there has been a change in ownership of the Service Provider or an Information Security Breach involving Service Provider.
 - d. Promptly upon receipt of Company's written request, Company may audit Service Provider Business Continuity Plan (BCP) and Disaster Recovery (DR) materials which pertain to or affect Company Information Assets, including BCP and DR plans and test results, at least annually, and following any man-made or natural disaster.
 - e. Service Provider attests that software and services provided under the Agreement, if any:
 - i. Does not contain undocumented features;
 - ii. Does not contain hidden mechanisms that could be used to compromise Company Information Assets;

- iii. Will not compromise, require modification of, disable or otherwise circumvent previously implemented information security controls.

7. **General Information Security Requirements.**

- a. Service Provider must ensure appropriate segregation of duties exist for all job functions and roles performed by its employees and Agents to ensure that no individual, within or external to Service Provider's organization, has conflicting duties that could jeopardize Company Information Assets.
 - b. Company Information Assets should not be divulged in any way to anyone without a specific valid business "need to know" and Company written authorization.
 - c. Access to all Company Information Assets must:
 - i. adhere to the principle of "least privilege," ensuring that only the most minimal level of access needed for a given job function of access is granted to Service Provider's employees and its Agents;
 - ii. be restricted to only authorized personnel who have a specific business "need to know."
 - d. Computer services employed to view, host, store, process, transmit, print, back-up or destroy Company Information Assets must adhere to the principle of "least privilege," ensuring that only the most minimal level of access needed to perform processing is granted to these computer services.
 - e. Hardware and software owned by Service Provider personnel must not be allowed to connect to or interact with the Company's company network without:
 - i. an appropriately scoped risk assessment, including the identification of existing and compensating controls based upon the requirements within this Attachment;
 - ii. verification of the implementation of controls identified within the risk assessment;
 - iii. obtained approvals of Company IT Network Management and the appropriate Chief Information Officer of the enterprise or division of Company involved.
 - f. Service Provider's users should not be allowed to install their own personal software on Service Provider Information Assets.
 - g. Service Provider portable devices that store, process, transmit or destroy Company Information Assets, such as laptops, personal digital assistants (PDAs), Blackberries^{*}, smart phones, hand-held or palmtop computers, portable memory drives, and other similar portable devices must be configured to make use of industry standard encryption technology that fully protects these devices' storage and transmission capabilities from unauthorized access.
8. **Information Asset Classification and Management.** Service Provider must classify and control its Information Assets to indicate the ownership, custodianship, and degree of sensitivity consistent with Company's Information Asset classification in order to ensure that Company Information Assets receive an appropriate level of protection by Service Provider. The inventory of Service Provider's Information Asset classification repository must be maintained and kept current. Recommended classifications are as follows:
- a. Non-sensitive Business Data and Public Information Assets (Public Release)
 - i. "Non-sensitive Business Data" refers to all Information Assets determined by Company to not be sensitive or confidential as defined below;

- ii. "Public Information" refers to all Information Assets that comes from public sources or is provided by Company to the general public; examples include periodicals, public bulletins, published company information, published press releases, etc.
- b. Confidential and Proprietary Company Information Assets (Confidential)
 - i. "Confidential" or "Proprietary Information Assets" refers to Information Assets that are internal to Company, though it may be shared with Service Provider under the terms of the Agreement, and are not considered by Company to be Public Release; examples include unpublished corporate financial information, information about impending mergers and acquisitions, dormant account information, marketing plans, passwords and encryption keys, employee and customer non-public personal information (such as personally identifiable information, personal financial information or personal protected health information), product designs, customer records and correspondence, and other information or data which if disclosed without appropriate authorization could result in a competitive disadvantage or liability or loss to the Company.
 - c. Record retention periods that meet federal and state retention requirements must be established and maintained by Service Provider. In addition, the Parties may agree in writing to specific retention requirements that Service Provider will follow, including but not limited to, retention for compliance, litigation, legal or regulatory purposes.
 - d. Destruction of Company Information Assets must not occur outside of the agreed upon retention schedule without authorization from Company management. The destruction methodologies must be performed in a secure manner such that the information cannot be read or re-created after disposal. Service Provider is encouraged to adhere to the guidelines provided by the National Association for Information Destruction (NAID), which can be found at <http://www.naidonline.org>. Service Provider must also take into consideration the impact of disposal on the environment.
 - e. At Company's expense, promptly upon receipt of Company's written request, Service Provider will work with Company to return all Company Information Assets in a reasonable manner and timeframe, taking into consideration then current technologies and industry best practices for information transfer and asset transportation, ensuring at a minimum that the information is either destroyed according to Company requirements or returned to Company in a format that is reasonably organized and usable by Company. However, if such return is infeasible, Service Provider will limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible and extend the provisions of this agreement as long as the information is maintained. Where errors in data transfer exist, Service Provider agrees to work with the Company to provide reasonable effort to correct problems with the integrity of transferred data.
- 9. **Human Resources Management.** The following administrative requirements must be implemented by Service Provider where Company Information Assets are stored, processed, transmitted, or destroyed; except as may be otherwise required for compliance, litigation or legal or regulatory purposes.
 - a. Service Provider employees and Agents must be subject to a sufficient criminal background check prior to employment to ensure people with a criminal history do not have access to Company Information Assets. The Service Provider agrees it will provide no employees or Agents who have been convicted of a felony involving theft, dishonesty, or breach of trust, or any other crime that disqualifies someone from working in the business of insurance as set forth in the Federal Crime Bill. Further, Service Provider will conduct a background check on each employee or Agent that is sufficient to screen out those who have been convicted of crimes involving behavior that, if it occurred on the Company's site, could result in injury to people or impairment of assets.

- b. Service Provider must follow a documented method or procedure that governs the creation, suspension, cancellation, modification, and deletion of user accounts for its employees and Agents. These methods or procedures must include, at a minimum, the following:
 - i. Employees and Agents with valid user accounts must have their user accounts disabled immediately upon termination of employment or business engagement;
 - ii. Employees and Agents who experience an absence longer than ninety (90) days must have their user accounts disabled. These user accounts may be re-enabled upon their return to work; otherwise, these accounts shall be deleted upon termination of the Employee or Agent;
 - iii. Employees and Agents whose job responsibilities change must have their access levels reviewed to determine if changes need to be made in order to ensure they do not have access to Information Assets for which they do not have a specific business need.
- c. During employment or when under contract:
 - i. Service Provider must include Information Security requirements within job descriptions or other written documentation for Service Provider employees and Agents whose job roles will have access to Company Information Assets;
 - ii. Service Provider must maintain an Information Security awareness and training program for its employees and Agents to ensure the employees and Agents are aware of their responsibility to protect and maintain the confidentiality and security of Service Provider and Company Information Assets;
 - iii. Service Provider shall impose disciplinary measures for violations of its Information Security Program.
- d. Upon termination of employment or contract:
 - i. Service Provider shall notify Company in writing within 24 hours when Service Provider's employees and Agents who have access to Company's network and internal systems are reassigned and no longer need access, or are no longer working for Service Provider, thereby enabling Company to remove access in a timely manner;
 - ii. Service Providers must secure all Company Information Assets within their custody from employees and Agents upon termination of employment or contract.

11. Physical Security.

- a. Access to Company Confidential Information Assets must be controlled to protect the confidentiality, integrity, and availability of Company Confidential Information Assets with appropriate administrative, logical, and physical safeguards, including but not limited to:
 - i. locking office doors;
 - ii. securing storage containers; and
 - iii. shredding or otherwise securely destroying Information Assets at appropriate times.
- b. Physical entry to Service Provider's premises must be controlled such that unauthorized entry is prevented, detected and reported to appropriate Service Provider personnel immediately. All entry and exit points must be secured, logged and monitored to ensure only authorized personnel may gain entry to Service Provider's buildings and secured areas.

- c. Where Service Provider has utilized identification badges or similar tokens for its employees and Agents, a documented process must exist, along with supporting procedures, to ensure lost badges and tokens are disabled immediately upon notification of the loss.
- d. When a Service Provider employee or other Agent is terminated, procedures must exist to ensure the identification badges are immediately disabled.
- e. All Company Information Assets in Service Provider's possession must be physically secured in an access-controlled area, in a locked room, or secured storage container or file cabinet.
- f. Company Information Assets must not be removed from Service Provider's premises without written consent from Company and written authorization from Service Provider management.
- g. All Company Information Assets, together with Service Provider Information Assets used to provide services to Company, must be protected to minimize the risk of physical and environmental threats that could jeopardize Information Asset confidentiality, integrity, and availability.
- h. Physical access to computer sessions must be secured when a user who is actively logged into session is not physically present to monitor activity and viewing of Information Assets displayed within that session. Examples of physical controls include, but are not limited to:
 - i. utilizing screen savers which lock the screen and keyboard access after a short period of inactivity;
 - ii. manually locking the keyboard;
 - iii. physically securing the office where the computer resides;
 - iv. positioning the monitor away from an unauthorized view.
- i. **Information Back-up.**
 - i. Adequate backup facilities should be provided to support the recovery of Company Information Assets in accordance with Company disaster recovery requirements and record retention schedules. Minimal requirements include:
 - ii. Media containing back-up copies of Confidential and Proprietary Company Information Assets should be encrypted using industry standard methods to conceal these Information Assets from unauthorized access;
 - iii. The back-up storage media used to store Company Information Assets must be of a type that has been determined by Service Provider to be appropriate for the confidentiality and retention requirements of the data it will contain;
 - iv. As it is critical that the back-up storage media be machine readable in the event it is needed for restore and recovery operations, random controlled testing of the restoration process must occur;
 - v. Back-up copies of Company Information Assets, together with complete and accurate records of the back-up copies, must be stored at a physically secured offsite location as a measure of protection against total loss of Information Assets in the event of a system failure or disaster;
 - vi. Company Information Assets should be backed up on a schedule that aligns with disaster recovery requirements. This schedule includes requirements for weekly full backups, daily incremental backups, quarter end backups and year end backups;

- vii. No more than one (1) full back-up and six (6) days of subsequent incremental back-ups may be stored on Service Provider premises at any time.
- j. **Network Security.**
 - i. Company may terminate any network or other Remote Connection with Service Provider at any time without warning if it is suspected or confirmed that any such connection is not secure.
 - ii. Company Information Assets must not exist on any computer or device that is directly exposed to the Internet or other non-Service Provider network, unless specifically authorized by Company in writing.
 - iii. Service Provider shall establish and maintain appropriate controls for its electronic interfaces and connections between its own systems and those of others (Remote Connections) utilizing industry best practices.
 - iv. Devices must be verified prior to connecting to the Company or Service Provider network segments where Company Information Assets reside to comply with the following hardening requirements to protect from compromise:
 - v. Devices must employ an antivirus and file integrity checking system with:
 - 1. A method for updating antivirus definition information to be current at all times;
 - 2. Enabled real-time antivirus scanning of system activity, including all accessed files and memory;
 - 3. Scheduled weekly full directory and file antivirus scan;
 - vi. Devices must employ up-to-date system software, including but not limited to, up-to-date system software patches and security updates.
 - vii. Devices must employ a firewall, proxy or other network traffic filtering technology to deny invalid in-bound traffic to and reasonably protect out-bound traffic from that device;
 - viii. System logs or equivalent tracking software must be configured to reasonably capture common errors and invalid access attempts;
 - ix. The integration of new software on devices granted connectivity permission must be preceded by a risk assessment and incorporate formal change control procedures to determine and protect the impact to the Company network.
 - x. Permission to connect any device to the Company network shall be proceeded by:
 - 1. A Company risk assessment to determine the impact to the Company network;
 - 2. Approvals from Company, including its IT network manager, impacted technical IT managers, and a divisional Chief Information Officer or his/her designee; and
 - 3. Service Provider networks must have firewalls deployed at the network perimeter to deny unauthorized in-bound and appropriate out-bound network traffic from the Internet and other non-Service Provider networks.

- xiii. Service Provider applications and systems that view, host, store, process, transmit, print, back-up or destroy Company Information Assets must be logically segregated from other systems on the Service Provider internal network by an appropriate firewall- or proxy-based, or similar, architecture that will disallow unauthorized in-bound and out-bound connections to Company Information Assets.
- xiv. Intrusion detection systems (IDS) or intrusion prevention systems (IPS) must be in place to provide reasonable logging and protection against malicious network activity. These systems should be configured to alert appropriate information security and information technology personnel who will then bear the responsibility to take action to disallow said network activity from affecting Company Information Assets.
- xv. Unattended network ports must be secured or disabled when not in use. Where business requirements justify the need, network ports may remain active provided that Service Provider management has reviewed the business need and there is documented approval. Examples of such need would include network ports in conference rooms, shared work areas, etc.
- xvi. Wireless network access points must be configured to ensure that only authorized Service Provider devices may establish a connection to the Service Provider internal network where Company Information Assets are viewed, hosted, stored, processed, transmitted, printed, backed-up or destroyed. Further, the wireless network connections established must utilize industry best practices for encryption and other appropriate safeguards designed to protect against unauthorized access and use.

k. System Event Logging, Monitoring, and Reporting.

- i. Service Provider computer and network systems used to provide services to Company must log significant events including, but not limited to, the following:
- ii. Unauthorized attempts to access Service Provider network or Company Information Assets must be captured and securely logged in such a way to support error handling and forensic needs.
- iii. Logs must be configured or secured such that they cannot be viewed or altered by anyone without authorization, including those with administrative privileges, unless such access is also logged in a tamper-evident manner;
- iv. Logs of unsuccessful login attempts to network and unsuccessful access to Information Assets must be reviewed on a regular basis to detect and appropriately act upon anomalous and suspicious system access attempts;
- v. When suspicious or anomalous activity is detected during a review of the aforementioned logs, it should be reported as directed by approved event handling procedures aligning with Information Security Incident Response plans.

l. Logical Access.

- i. All computer-based information systems connected to any portion of the Service Provider network where Company Information Assets are located or processed must employ, at a minimum, the following requirements:
- ii. Service Provider shall grant access to each user on a personally identifiable unique user account;
- iii. Wherever technically possible, the password settings for each user account must be configured using the following minimal configuration:

1. Minimum of eight (8) characters in length and contain characters from at least three (3) of the following four (4) character types:
 - a. upper case alpha characters;
 - b. lower case alpha characters;
 - c. numeric characters;
 - d. special characters (e.g., !, \$, @, etc.).
2. Expiration of password must be minimally set as follows:
 - a. Set to automatically require password changes, at a maximum, every sixty (60) days, for user accounts and any system account where the setting will not hinder production processing;
 - b. If the automatic expiration of a system account would potentially cause the risk of interruption of production processing, password changes may occur manually with the following alternate controls in place:
 - (i) The system account is assigned a unique owner who is ultimately responsible for the disposition and usage of the account and password;
 - (ii) The system account is configured with advanced complex password creation rules (e.g., extended password length, hashing algorithms, etc.);
 - (iii) The system account is limited wherever possible to allow log on capabilities only to required computers and/or services;
 - (iv) The system account is changed manually at least once a year and upon turnover of staff at the earliest time available so as not to affect processing;
 - (v) The system account complies with all other requirements within this Attachment.
 - iv. The password settings for each vendor-supplied default account must be changed and configured using the minimal configuration outlined in this 14. a. ii.
 - v. Accounts with any access to Company Information Assets must be configured wherever technically possible to disallow login capability after a maximum of seven (7), unless otherwise required to be a lesser number (e.g., PCI, etc.), consecutive unsuccessful login attempts.
 - vi. Stored password text must be stored in an encrypted form in the user identity database, and they must be rendered unreadable during transmission and storage (e.g., appropriately concealed within strongly restricted directories, etc.) if embedded within batch files, automatic login scripts, software macros, terminal function keys, on computers where access controls are otherwise disabled, or any location where unauthorized individuals might discover them.
 - vii. Passwords must be changed immediately if it is discovered that they are disclosed to or discovered by unauthorized parties.
 - viii. Service Provider systems must be configured wherever technically possible to disable user sessions after a reasonable period of inactivity, based upon business risk.
 - ix. Additional and/or stronger logical access safeguards may be implemented by Service Provider at its discretion, so long as such additional controls do not neutralize nor negate the effectiveness of existing controls for Company Information Assets as outlined within this Attachment.

m. System Development.

- i. Application and system development must follow a defined and documented systems development life cycle (SDLC) methodology that includes a preliminary review of information security requirements to ensure, at a minimum, the following:
 - ii. Vulnerability testing must be performed to ensure common security weaknesses are detected and corrected prior to being implemented;
 - iii. There must be separate physical or logical environmental partitions separating development, test, staging and production environments;
 - iv. The use of data within non-production environments must adhere to the following at a minimum:
 1. Wherever possible, fictitious data based upon real data cases must be employed in test environments;
 2. If Company Information Assets are used, the same controls must exist as within the production environment;
 3. If Company Information Assets are used, it must be immediately removed from all non-production environments upon the completion of its use;
 4. Handling and destruction of sensitive non-production data and output must be treated as the same level of confidentiality as if it were production;
 - v. Logical access controls must be defined, tested and incorporated to ensure they work as designed and support the ability to restrict access to only those Company Information Assets required for Service Provider and Company business requirements, while also supporting the principle of least privilege;
 - vi. Segregation of duties must be incorporated into the design of applications and systems to prevent the ability of a single person to perform multiple functions that could lead to fraud, theft, or other illicit or unethical activity through the use of the functions of the applications and systems where Company Information Assets are stored, processed, transmitted, or destroyed;
 - vii. Web-based applications exposed to the Internet must ensure vulnerability testing is performed to ensure the most common vulnerability weaknesses based upon industry best practices are identified and remediated to prevent them from being exploited in a way that could lead to unauthorized access to or disclosure of Company Information Assets;
 - viii. A formal, documented change management process must be used when making changes to applications and systems that view, host, store, process, transmit, print, back-up or destroy Company Information Assets. This change management process must, at a minimum, include the following:
 1. Each change must be reviewed and approved by Company management. Changes to applications and systems must not be deployed into production environments by the same people who do the development and quality assurance of applications and systems;
 2. A record of all changes to applications and systems must be maintained that identifies:
 - a. a brief description of each change that was made;
 - b. who made each change;
 - c. test plans and results for each change;

- d. who approved each change;
- e. when each change was made.

n. Information Security Incident Response and Breach Notification.

- i. Service Provider must establish and maintain a documented Information Security Incident Response program (ISIRP) that includes, at a minimum, the following:
 - ii. Service Provider must define and document the roles and responsibilities of its ISIRP team members;
 - iii. Service Provider ISIRP team members must receive training at least annually to ensure they understand what to do during an Information Security event or incident;
 - iv. Service Provider must establish and maintain a documented set of procedures and notification requirements to follow that provides guidance to the ISIRP team when responding to an event or incident;
 - v. Procedures and other documentation must provide guidance to the ISIRP team regarding Information Security event and incident records. All relevant event and incident logs, along with any related notes of actions taken in response to these events and incidents, must be secured and retained, based upon an approved retention schedule;
 - vi. Any unmitigated Information Security Breach experienced by Service Provider prior to the execution of the Agreement must be disclosed to Company.
 - vii. Any actual or suspected Information Security Breach experienced by Service Provider involving Company Information Assets must be reported to Company within forty-eight (48) of its detection. A formal communication plan for notification must be defined and documented between the parties. The parties agree to reasonably coordinate and cooperate with each other in investigating the suspected breach. Service Provider shall take immediate steps to remedy the Information Security Breach at Service Provider's expense in accordance with applicable privacy rights and laws. Service Provider shall reimburse Company for actual costs incurred in responding to/and or mitigating damages caused by an Information Security Breach. For purposes of the Service Provider's reimbursement obligation in the preceding sentence, Service Provider shall only be obligated to reimburse a reasonable amount of Company's costs based upon the nature of the Security Breach, the size of the Security Breach and the number of individuals impacted by the Security Breach.

o. Business Continuity.

- i. Business continuity recovery point objectives (RPO) and recovery time objectives (RTO) must be discussed with Company and agreed to commensurate with the execution of the Agreement. This is done to ensure Service Provider recovery capabilities and subsequent commitments to do so will meet Company's business requirements.
- ii. Service Provider or Agent shall maintain a documented business continuity and disaster recovery (BCP/DR) plan which, at a minimum, must:
 - ii. Govern and define the objectives and actions required during a BCP/DR event;
 - iii. Secure offsite copies of appropriate business continuity and disaster recovery documentation for retrieval in a reasonable time period by those who will need access to this information following a disaster event;

- iv. Define and document business continuity processes and procedures to enable Service Provider to perform the actions necessary to maintain critical business functions following a disaster event;
 - v. Define and document Information Asset disaster recovery procedures to enable Service Provider to recover Company Information Assets in a manner consistent with established and agreed upon RPO and RTO business continuity requirements;
 - vi. Prioritize recovery activity based upon a documented inventory of Company Information Assets in accordance with the established and agreed upon RPO and RTO;
 - vii. Define and document a formal communication plan to require that notification of any BCP/DR invocation be provided to Company within one (1) full business day of its occurrence.
- p. **Compliance.**
- i. Service Provider must comply with all applicable international, state, federal, and private industry regulatory and statutory requirements. Examples of some of these requirements include, but are not limited to, adherence to the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA).
 - ii. Unlicensed and/or unapproved software must not be used on any Company Information Asset or on Service Provider Information Assets.
 - iii. All software installed on Service Provider Information Assets must be approved by appropriate Service Provider management to ensure it satisfies a business need, configured to conform to the principle of "least privilege," and is in compliance with applicable technical and information security requirements.

EXHIBIT C
UNDERWRITING SERVICES

General Service Levels: Service Provider shall adhere to the following general requirements:

- * Company may allow transitional Service Levels for up to 3 months upon launch of new Service Provider to manage acclimation and adjustments.
 - Documents will be transmitted/provided in Company's standard image and data format, if applicable. If Service Provider cannot transmit images and data per Company's standard format request, then this Exhibit C will be amended to identify the mutually agreed-upon format for such transmissions.
 - Service Provider shall provide reporting to support adherence to applicable Service Levels as set forth in this Agreement, as well as on an ad hoc basis. Monthly reporting due by the 8th of each month for prior month's Service Level performance results.
 - Service Provider shall report Services received, canceled and completed on a monthly basis in accordance with the defined Service Levels within this Agreement in a format acceptable to all parties.
 - Service Provider will provide ad hoc reporting as needed or agreed upon.
 - Service Provider to provide a written Root Cause Analysis (RCA) & Remediation Plan by 10th day of month following failure to meet a Service Level Standard.
 - Service Provider will provide Company with copy (images) of Services within 2 business days of Services being completed.
 - Service Provider will maintain web sites linked to the Company's systems (when applicable), or external websites that provide both ordering and status functions. Service Provider will provide secured access including User ID's and Password management for Company employees as needed.
 - Service Provider will provide electronic ordering and status functions in data format as mutually agreed upon in writing.
 - Service Provider shall notify Company of any complaints received from customers of Company and/or Service Provider within 2 business days of notification. Additional historic or substantiating information needed for Company to assess complaint will be provided within 1 business day from Company's request.
 - Service Provider shall perform a quality assurance check a minimum of 5% of Services on a monthly basis. Results of the quality assurance check to be provided to the Company on a monthly basis for the prior month's quality results.

- Company reserves the right to audit Service Providers quality assurance process and results without cause upon ten (10) business days' notice. When requested, Service Provider will cooperate by providing information for Services selected by Company for such quality assurance reviews/audits.
- Service Provider shall discount specific line of Services by 5%, if not remedied for 3 consecutive months, for any month that Service Levels are not met which will be credited on the month following missed Service Levels. (For example, Service Level missed January, February and March, will cause 5% of the March invoice to be credited to Company's April invoice)
- Service Provider shall utilize only Company approved letters, e-mails and scripts when contacting Company's customers, applicants and/or producers.

Telephone Interviews (“Interview(s)”) - Service Provider shall perform the following Services, and shall meet or exceed Service Level Standards with respect to all Interviews:

- Contact the applicant by telephone as required by Company within twenty-four (24) hours of Company's request. Subsequent contacts should be at the rate of five (5) attempts in three (3) days should the Company provide new information / telephone number.
- Service Provider shall complete the Interview, which shall consist of mutually-agreed upon questions and reflex questions.
- The average service time (measured from the time and date the Service Provider receives Company's request to conduct the Interview until the time and date the Company receives the Interview, including all delays), computed on a monthly basis, will be five (5) or less business days, unless delayed by applicant or agent, 95% of the time; 100% of Interview requests will be delivered within 7 business days (unless scheduled over 7 days in advance or later date requested by applicant.)
- Service Provider shall remit completed Interviews to Company or otherwise notify Company that interview cannot be completed and the reason therefore.
- Interviews not completed within this time frame will remain open for a period of 45 days before being closed for billing; this is so that the applicant may call in to complete the interview without the need of placing a new order.
- Service Provider shall provide average length of interview on a semi-annual basis.

Face-to-Face or Paramedical Assessments (“Assessment(s)”) - Service Provider shall perform the following Services, and shall meet or exceed the following Service Level Standards with respect to all Assessments:

- Make appointment with the applicant for an Assessment at a reasonable hour as requested

by approved Company producers and/or by Company. Initial contact with the applicant will take place within two (2) business days of Company's request.

- Service Provider shall visibly display credentials during appointment and shall dress in a manner consistent with the professional service being completed.
- Service Provider shall ensure that all blood samples are kept cool and centrifuged within 4 hours of collection. All applicable fees for Services billed for applicants wherein fluid collection was handled improperly shall be deducted.
- Service Provider shall use best efforts to ensure that all medical information supplied by applicant has relevant details which include dates, diagnosis, outcome and any follow-up. Company may deduct 50% of all applicable fees for Services billed whereby relevant details are omitted by Service Provider.
- The average service time (measured from the time and date the Service Provider receives Company's request to conduct the Assessment until the time and date the Company receives the Assessment, including all delays), computed on a monthly basis, will be fourteen (14) or less calendar days 80% of the time; 90% of Assessment requests will be delivered within 28 calendar days (unless scheduled at a later date as requested by applicant.)
- Service Provider shall remit completed Assessment to Company or otherwise notify Company that assessment cannot be completed and the reason therefore.

Attending Physicians' Statements ("APS") - Service Provider shall perform the following Services, and shall meet or exceed the following Service Level Standards with respect to all APS:

- All APS requests will be accompanied by proper authorizations signed by the Company.
- Request, follow up, receive and forward copies of medical records from the physician, clinic or medical facility as requested by approved Company producers and/or from Company.
- 95% of all requests will have initial contact with the physician, clinic, or medical facility attempted no later than 1 business day following receipt of order; 99% of all requests will have initial contact with the physician, clinic, or medical facility attempted no later than 2 business days following receipt of order.
- Remit completed APS to Company or otherwise notify Company that APS cannot be completed and the reason therefore.
- Service Provider will report percentage of APS completed in > 14 calendar days, 21 calendar days, 28 calendar days and percentage completed over 28 calendar days.

- The average service time (measured from the time and date the Service Provider receives Company's request for APS until the time and date that Company receives the APS), computed on a monthly basis, will be fourteen (14) or less calendar days.
- No less than 65% completed within 14 calendar days. No less than 75% completed within 21 calendar days. And no less than 90% completed within 28 calendar days.

EXHIBIT D
Underwriting Services and Fees

Paramedical Services

Service Name	Service Codes	Price	Kit Cost	Kit Handling
Paramed Exam Only	2	\$42.75	NA	NA
Paramed, Blood and Urine	2+29	\$68.40	\$8.30	\$5.75
Paramed, ECG, Blood and Urine	2+123+29	\$96.90	\$8.30	\$5.75
Paramed and Blood	2+29	\$68.40	\$8.30	\$5.75
Paramed and EKG	2+123	\$71.25	NA	NA
Paramed and Urine	2	\$42.75	\$5.00	\$5.75
Paramed, DBS and Urine	2+5084	\$68.40	\$8.30	\$5.75
Paramed, EKG and Urine	2+123	\$71.25	\$5.00	\$5.75
Medical Exam Only	1	\$85.50	NA	NA
Medical, Blood and Urine	1+61	\$129.20	\$8.30	\$5.75
Medical, EKG, Blood and Urine	1+14+61	\$161.50	\$8.30	\$5.75
Medical, Blood, Urine and Treadmill	1+31+61	\$570.00	\$8.30	\$5.75
Medical and EKG	1+14	\$117.80	NA	NA
Medical and Treadmill	1+31	\$526.30	NA	NA
2 Urine collections on different days	283	\$70.30	\$10.00	\$5.75
Blood Draw and EKG	1198	\$71.25	\$8.30	\$5.75
Blood Draw Only	1018	\$42.75	\$8.30	\$5.75
Blood Draw with Stats (HT, WT, BP, Pulse)	1120	\$50.00	\$8.30	\$5.75
Urine Only (includes Recheck)	15	\$36.10	\$5.00	\$5.75
DBS Collection Only	5085	\$38.00	\$8.30	\$5.75
EKG Only	4	\$54.15	NA	NA
EKG with Blood, Urine and Stats (HT, WT, BP, Pulse)	1120+123	\$78.50	\$8.30	\$5.75
Oral Fluid Only	409	\$36.10	\$7.70	\$5.75
Blood Pressure Only	156	\$34.75	NA	NA
Blood Pressure Readings on 2 consecutive days	5	\$69.65	NA	NA
Physical Measurements (HT, WT, BP, Pulse)	23	\$34.20	NA	NA
Weight and Height Recheck	23	\$34.20	NA	NA
IGO Mobile	6000	\$11.50	NA	NA
Packet Take out	490	\$7.70	NA	NA
Cancellation Refusal at Door	19	\$23.75	NA	NA

Average Price of Gas Per Gallon	Surcharge
\$2.74 or less	\$0
\$2.75 - \$3.24	\$1.50
\$3.25 - \$3.74	\$2.00
\$3.75 - \$4.24	\$2.50
Above \$4.25	TBD

When the price of gas exceeds \$2.75 per gallon
Company will pay a fuel surcharge. 100% of this fuel
surcharge is allocated back to the examiner to defray
their fuel cost.

Rate Exceptions

Hawaii, Puerto Rico, Alaska and Guam 2 times above rate.

New York City, Nassau and Suffolk Counties, Boston, District of Columbia, California and Chicago 1.25 times above rate.

Medical Records

Service	2014 Price
APS Flat Rate*	\$50.00
Cancel/No Records	\$15.00
Rush Handling	\$10.00
Special Handling	Included

* The \$50.00 flat fee is to cover facility fees up to \$100.00. Fees in excess of \$100.00 require Home Office approval.

If fee approval is given, billed amount will be equal to the flat fee (\$50.00) plus the amount over \$100.00.

Interviews

Script Name	Report	Report Number	Rate Standalone	Rate w/report
PHI FE (old 45& over)	FR	1	\$22.35	n/a
PHI SR (old Final Expense 44&under)	FR	2	\$30.40	n/a
Transamerica Health Interview	FR	3	\$25.70	n/a
PHI-SI	FR	4	\$12.40	n/a
MedSup	FR	5	\$24.70	n/a
Juvenile	FR	6	\$18.10	n/a
LTC	FR	TBD	\$23.75	n/a
Agent Quality	QN	1	\$8.00	\$2.75
Disability Questionnaire	QN	2	\$8.00	\$5.25

Script Name	Report	Report Number	Rate Standalone	Rate w/report
Anemia Questionnaire	QN	5	\$8.00	\$6.25
Arthritis Questionnaire	QN	6	\$8.75	\$7.00
Back and Neck Pain Questionnaire	QN	7	\$10.25	\$8.00
Cancer Questionnaire	QN	8	\$8.25	\$6.25
Cerebral Palsy Questionnaire	QN	9	\$8.00	\$3.25
Diabetes Questionnaire	QN	10	\$10.25	\$8.00
Depression, Mental & Nervous Disorder	QN	11	\$10.75	\$8.50
Gastrointestinal Questionnaire	QN	12	\$8.75	\$7.00
Heart Disease/Disorder Questionnaire	QN	13	\$9.50	\$7.50
Heart Murmur Questionnaire	QN	14	\$8.00	\$5.75
Hepatitis Questionnaire	QN	15	\$11.50	\$9.00
Hysterectomy	QN	16	\$8.00	\$4.25
High Blood Pressure Questionnaire	QN	17	\$8.25	\$6.25
Lupus Questionnaire	QN	18	\$8.00	\$5.75
Multiple Sclerosis Questionnaire	QN	19	\$8.75	\$7.00
Pregnancy	QN	20	\$8.00	\$4.25
Respiratory Disorder Questionnaire	QN	21	\$8.25	\$6.25
Seizure Questionnaire	QN	22	\$10.75	\$8.50
Skin Cancer Questionnaire	QN	23	\$8.00	\$5.75
Sleep Apnea Questionnaire	QN	24	\$8.75	\$7.00
Stroke Questionnaire	QN	25	\$9.50	\$7.50
Thyroid Questionnaire	QN	26	\$8.00	\$5.25
Ulcer Questionnaire	QN	27	\$8.00	\$5.25
Occupation and Income	QN	28	\$8.00	\$4.75
Foreign Travel	QN	29	\$8.00	\$1.75
Military	QN	30	\$10.75	\$8.50
Tobacco Questionnaire	QN	31	\$8.00	\$1.05
Alcohol-Drug Questionnaire	QN	32	\$8.00	\$5.75
Driving Questionnaire	QN	33	\$8.00	\$4.25
Aviation	QN	34	\$14.25	\$11.00
Avocation	QN	35	\$11.50	\$9.00
NY Avocation	QN	36	\$11.50	\$9.00
MD Avocation	QN	37	\$10.75	\$8.50
FL Avocation	QN	38	\$10.75	\$8.50
Residency	QN	40	\$8.00	\$4.75
Close out/Cancellation	N/A	N/A	\$5.40	N/A
Language Line	N/A	N/A	Varies	N/A
Additional SI Questions	SR	99	See Note	N/A
Special Instructions Questions Only	SR	99	\$8.00	NA

Script Name	Report	Report Number	Rate Standalone	Rate w/report
General Medical Follow Up Questions**	QN	4	n/a	\$3.25

*Used by Company for specific questions. Max. 3 questions.

** This will only bill when a medical question is answered "Yes" in the 10 Year Medical HX section.

Inspection Reports

Service	2014 Price
Quick E-Search	\$12.20
Amplified with Source	\$40.05
Bus Amp w/Source	\$53.05
Business Beneficiary	\$34.80
Credit Report	\$10.25
Bankruptcy	\$10.25
Criminal Records*	\$23.30
*Criminal records have a fee assessed by the county that may apply as a pass thru fee	Varies
^Close Out - Includes cancellation/close out fee plus credit report	\$15.00
Language Line	Varies

[^]The credit report is ordered upon receipt. All close outs will include credit report since it is ordered prior to interview

EXHIBIT 2

STATE OF TEXAS }
COUNTY OF DALLAS }

I, FELICIA PITRE, Clerk of the District of Dallas County,
Texas, do hereby certify that I have compared this instrument
to be a true and correct copy of the original as appears on
record in my office.

GIVEN UNDER MY HAND AND SEAL of said Court, at office
In Dallas, Texas, this 11th day of Sept., A.D., 2020.

FELICIA PITRE, DISTRICT CLERK
DALLAS COUNTY, TEXAS
By Michael E. Clark Deputy

Michael Earl Clark

CIVIL CASE INFORMATION SHEET

CAUSE NUMBER (FOR CLERK USE ONLY): DC-20-12059

COURT (FOR CLERK USE ONLY): _____

STYLED Money Services, Inc. v. Examination Management Services, Inc., EMSI Holding Company, RDI Xtract, LLC, RDI Corporation

(e.g., John Smith v. All American Insurance Co; In re Mary Ann Jones; In the Matter of the Estate of George Jackson)

A civil case information sheet must be completed and submitted when an original petition or application is filed to initiate a new civil, family law, probate, or mental health case or when a post-judgment petition for modification or motion for enforcement is filed in a family law case. The information should be the best available at the time of filing.

1. Contact information for person completing case information sheet:		Names of parties in case:	Person or entity completing sheet is:
Name: Susan E. Egeland	Email: susan.egeland@faegredrinker.com	Plaintiff(s)/Petitioner(s): Money Services, Inc.	<input checked="" type="checkbox"/> Attorney for Plaintiff/Petitioner <input type="checkbox"/> Pro Se Plaintiff/Petitioner <input type="checkbox"/> Title IV-D Agency <input type="checkbox"/> Other: _____
Address: 1717 Main Street, Suite 5400	Telephone: 469-357-2500	Defendant(s)/Respondent(s): Examination Management Services, Inc., EMSI Holding Company, RDI Xtract, LLC, RDI Corporation	Additional Parties in Child Support Case: _____
City/State/Zip: Dallas, TX 75201	Fax: 469-327-0860	Custodial Parent: _____	
Signature: /s/ Susan E. Egeland	State Bar No: 24040854	Non-Custodial Parent: _____	
[Attach additional page as necessary to list all parties]			

2. Indicate case type, or identify the most important issue in the case (select only 1):

Civil			Family Law	
Contract	Injury or Damage	Real Property	Marriage Relationship	Post-judgment Actions (non-Title IV-D)
<input type="checkbox"/> Debt/Contract <input checked="" type="checkbox"/> Consumer/DTPA <input type="checkbox"/> Debt/Contract <input type="checkbox"/> Fraud/Misrepresentation <input checked="" type="checkbox"/> Other Debt/Contract: <input type="checkbox"/> Foreclosure <input type="checkbox"/> Home Equity—Expedited <input type="checkbox"/> Other Foreclosure <input type="checkbox"/> Franchise <input type="checkbox"/> Insurance <input type="checkbox"/> Landlord/Tenant <input type="checkbox"/> Non-Competition <input type="checkbox"/> Partnership <input type="checkbox"/> Other Contract: 	<input type="checkbox"/> Assault/Battery <input type="checkbox"/> Construction <input type="checkbox"/> Defamation <i>Malpractice</i> <input type="checkbox"/> Accounting <input type="checkbox"/> Legal <input type="checkbox"/> Medical <input type="checkbox"/> Other Professional Liability <input type="checkbox"/> Motor Vehicle Accident <input type="checkbox"/> Premises <i>Product Liability</i> <input type="checkbox"/> Asbestos/Silica <input type="checkbox"/> Other Product Liability List Product: <input type="checkbox"/> Other Injury or Damage: 	<input type="checkbox"/> Eminent Domain/ Condemnation <input type="checkbox"/> Partition <input type="checkbox"/> Quiet Title <input type="checkbox"/> Trespass to Try Title <input type="checkbox"/> Other Property: 	<input type="checkbox"/> Annulment <input type="checkbox"/> Declare Marriage Void <i>Divorce</i> <input type="checkbox"/> With Children <input type="checkbox"/> No Children 	<input type="checkbox"/> Enforcement <input type="checkbox"/> Modification—Custody <input type="checkbox"/> Modification—Other Title IV-D <input type="checkbox"/> Enforcement/Modification <input type="checkbox"/> Paternity <input type="checkbox"/> Reciprocals (UIFSA) <input type="checkbox"/> Support Order
Employment	Related to Criminal Matters			Other Family Law
<input type="checkbox"/> Discrimination <input type="checkbox"/> Retaliation <input type="checkbox"/> Termination <input type="checkbox"/> Workers' Compensation <input type="checkbox"/> Other Employment: 	<input type="checkbox"/> Expunction <input type="checkbox"/> Judgment Nisi <input type="checkbox"/> Non-Disclosure <input type="checkbox"/> Seizure/Forfeiture <input type="checkbox"/> Writ of Habeas Corpus— Pre-indictment <input type="checkbox"/> Other: _____ 			<input type="checkbox"/> Enforce Foreign Judgment <input type="checkbox"/> Habeas Corpus <input type="checkbox"/> Name Change <input type="checkbox"/> Protective Order <input type="checkbox"/> Removal of Disabilities of Minority <input type="checkbox"/> Other:
Tax	Probate & Mental Health			
<input type="checkbox"/> Tax Appraisal <input type="checkbox"/> Tax Delinquency <input type="checkbox"/> Other Tax 	<i>Probate/Wills/Intestate Administration</i> <input type="checkbox"/> Dependent Administration <input type="checkbox"/> Independent Administration <input type="checkbox"/> Other Estate Proceedings <input type="checkbox"/> Guardianship—Adult <input type="checkbox"/> Guardianship—Minor <input type="checkbox"/> Mental Health <input type="checkbox"/> Other: 			

3. Indicate procedure or remedy, if applicable (may select more than 1):

<input type="checkbox"/> Appeal from Municipal or Justice Court	<input type="checkbox"/> Declaratory Judgment	<input type="checkbox"/> Prejudgment Remedy
<input type="checkbox"/> Arbitration-related	<input type="checkbox"/> Garnishment	<input type="checkbox"/> Protective Order
<input type="checkbox"/> Attachment	<input type="checkbox"/> Interpleader	<input type="checkbox"/> Receiver
<input type="checkbox"/> Bill of Review	<input type="checkbox"/> License	<input type="checkbox"/> Sequestration
<input type="checkbox"/> Certiorari	<input type="checkbox"/> Mandamus	<input checked="" type="checkbox"/> Temporary Restraining Order/Injunction
<input type="checkbox"/> Class Action	<input type="checkbox"/> Post-judgment	<input type="checkbox"/> Turnover
4. Indicate damages sought (do not select if it is a family law case):		
<input type="checkbox"/> Less than \$100,000, including damages of any kind, penalties, costs, expenses, pre-judgment interest, and attorney fees <input checked="" type="checkbox"/> Less than \$100,000 and non-monetary relief <input type="checkbox"/> Over \$100,000 but not more than \$200,000 <input type="checkbox"/> Over \$200,000 but not more than \$1,000,000 <input type="checkbox"/> Over \$1,000,000		

DC-20-12059

CAUSE NO. _____

MONEY SERVICES, INC.**Plaintiff,**

v.

**EXAMINATION MANAGEMENT
SERVICES, INC., EMSI HOLDING
COMPANY, RDI XTRACT, LLC, RDI
CORPORATION****Defendants.****IN THE DISTRICT COURT OF****DALLAS COUNTY, TEXAS****JUDICIAL DISTRICT COURT****PLAINTIFF'S ORIGINAL PETITION, APPLICATION FOR TEMPORARY
RESTRAINING ORDER, AND APPLICATION FOR TEMPORARY AND
PERMANENT INJUNCTIVE RELIEF****TO THE HONORABLE JUDGE OF SAID COURT:**

Plaintiff Money Services, Inc. ("MSI") files this Original Petition and, pursuant to equitable principles and Texas Rules of Civil Procedure 680, requests that this Court enter a temporary restraining order and temporary and permanent injunction against Examination Management Services, Inc. and EMSI Holding Company (collectively, "EMSI"), and RDI Xtract LLC ("RDI Xtract") and RDI Corporation (collectively, "RDI") that, among other relief, prevents or restrains EMSI and RDI from accessing, disclosing or otherwise allowing any third party to access MSI's Confidential Information and Proprietary Information, as those terms are defined in the Professional Services Agreement entered into between MSI and EMSI, as such access or disclosure will cause MSI immediate and irreparable harm with regard to its business. In support of its Original Petition and applications, MSI states:

**PLAINTIFF'S ORIGINAL PETITION, APPLICATION FOR TEMPORARY
RESTRAINING ORDER, AND APPLICATION FOR TEMPORARY AND
PERMANENT INJUNCTIVE RELIEF**

DISCOVERY CONTROL PLAN

1. MSI requests a Level 3 discovery control plan.

PARTIES

2. Money Services, Inc. is a corporation organized and existing under the laws of the State of Delaware, with its principal place of business located in Iowa. Money Services, Inc. provides services to its affiliated companies and divisions of such companies, including Transamerica Life Insurance Company.

3. EMSI Holding Company is a corporation organized and existing under the laws of the State of Delaware, with its principal place of business in Dallas County, Texas. Upon information and belief, Examination Management Services, Inc. is wholly owned and operated by EMSI Holding Company. EMSI Holding Company may be served with process by serving its registered agent, CT Corporation, 1999 Bryan Street, Suite 900, Dallas, Texas 75201.

4. Examination Management Services, Inc. is a corporation that provided ancillary services to the life insurance industry and is organized and existing with under the laws of the State of Nevada, with its principal place of business located in Dallas County, Texas. On July 3, 2020, EMSI abruptly, and without advance notice to MSI, ceased operations. Service on EMSI would be accomplished by serving its registered agent for service within the State of Texas: CT Corporation 1999 Bryan Street, Suite 900, Dallas, Texas 75201, by certified mail, return receipt requested. To further ensure notice and service, upon information and belief, communication with EMSI is presently limited to the following email address: board@emsinet.com, and service should also be permitted via this email address.

5. RDI Xtract is a corporation organized and existing under the laws of the State of Ohio. Upon information and belief, RDI Xtract acquired certain data servers and other equipment located in Irving, TX. RDI Xtract may be served with process by serving its Ohio statutory agent, Neil Desai, 4350 Glendale Milford Rd., Ste. 250, Cincinnati OH, 45242.

6. RDI Corporation is a corporation organized and existing under the laws of the State of Ohio with its principal place of business in Cincinnati, Ohio. Upon information and belief, RDI Corporation participated in the negotiations concerning the sale of EMSI's data servers and other equipment located in Irving, TX. RDI Corporation may be served with process by serving its Ohio statutory agent, George Trebbi, 4350 Glendale Milford Rd., Ste. 250, Cincinnati OH, 45242.

JURISDICTION & VENUE

7. The Court has jurisdiction over EMSI and RDI Xtract under the equitable principles and Texas Rule of Civil Procedure 680 and because the relief sought is within the jurisdictional limits of this Court. As required by Texas Rule of Civil Procedure 47(c)(4), MSI states that it seeks monetary relief of less than \$100,000, including damages of any kind, penalties, costs, expenses, and pre-judgment interest. MSI also seeks non-monetary relief, including specific performance under the Contract.

8. Venue is proper in Dallas County because a substantial part of the events or omissions giving rise to the lawsuit, including the location of the servers that store the data at issue, took place there. *See TEX. CIV. PRAC. & REM. CODE §§ 15.002(1), 15.005.* Upon information and belief, the servers storing the MSI's Proprietary Information are located at facilities in Irving, Texas.

OPERATIVE FACTS¹

9. On or about April 25, 2014, MSI and EMSI entered into a Professional Services Agreement (the “Contract”) to support the application and underwriting process for MSI’s affiliated companies’ life and long-term care insurance business.²

10. On July 3, 2020, EMSI abruptly, and without advance notice to MSI, ceased operations. According to EMSI’s current website: “COVID-19 has disrupted families, communities, and businesses in our country and around the world. EMSI has become a casualty of these unprecedented times, as the pandemic has severely depressed service volumes. As a result, all company operations ceased on Friday, July 3, 2020.” See <https://www.emsinet.com/>.

11. Around the time of its sudden closure, certain former employees at EMSI endeavored to partner with a competitor of EMSI, RDI Corporation, to market its services to EMSI’s former customers, including MSI. On July 6, 2020, Kamette Myers, a former EMSI employee responsible for client relationships, introduced by e-mail Linda McFadden, a Lead Vendor Manager at Transamerica based in Plano, Texas, to representatives of RDI Corporation to discuss the possibility of transitioning MSI’s business to RDI Corporation. On July 7, 2020, Matt Dowd, Senior Vice President of RDI’s Contact Center Operations, wrote to Ms. McFadden by e-mail and stated, “[i]f we can get past the contract details we are willing to bring the entire [Texas-based] EMSI team over to RDI including the managers who ran the account.”

¹ The factual allegations contained in this section are supported by the Unsworn Declarations of Linda McFadden and Susan Egeland in Support of Plaintiff’s Original Petition, Application for Temporary Restraining Order, and Application for Temporary and Permanent Injunctive Relief, which are attached hereto as Exhibit A and are incorporated herein by reference. Due to the Covid-19 related stay-at-home order in place at the time of this filing, Defendant’s counsel submits a Declaration in lieu of Affidavit pursuant to Texas Civil Practice and Remedies Code Section 132.001(a).

² A true and correct copy of the Contract, as amended and including all statements of work and orders, is attached hereto as Exhibit B.

12. Upon information and belief, RDI Corporation formed RDI Xtract as a wholly owned subsidiary on or around July 10, 2020, in part, to purchase certain assets from EMSI.

13. On July 30, 2020, RDI Xtract acquired certain assets from EMSI. Specifically, upon information and belief, RDI Xtract acquired EMSI's data servers and other equipment in connection with the transaction.

14. Upon information and belief, RDI induced or otherwise conspired with EMSI to sell MSI's Proprietary Information or otherwise transfer possession and control of such data to RDI Xtract in connection with the sale of the data servers, despite EMSI and RDI knowing that such data belonged to MSI and that a transfer to RDI Xtract would be in breach of the Contract and would prevent or otherwise interfere with EMSI's performance of its continuing obligations under the Contract.

15. Upon information and belief, RDI induced EMSI to sell EMSI's former clients' data, including MSI's data, for the purpose of RDI Xtract leveraging its possession and control of that data to market its services to EMSI's former clients, including MSI.

16. RDI marketed and continues to market its services to MSI and, upon information and belief, EMSI's other former clients.

MSI's Contract with EMSI

17. EMSI provided a host of services on behalf of MSI, including but not limited to telephone application interviews, the retrieval of patient medical records, and various lab and medical examinations (the "Services").

18. Under the Contract, Confidential Information is defined, in relevant part, as "information identified on, in or constituting: ... results of the Services, ... data, business records,

customer lists, policy information, [policyholder] information...and any and all other tangible or intangible information, other than Trade Secrets, ... which is generated or learned as a result of or in connection with the Services and is not generally available to the public.” *See Ex. B, at Section 1.4.*

19. Proprietary Information is defined to include Confidential Information and Trade Secrets furnished, transmitted to, observed or otherwise obtained by EMSI. *See Ex. B, at Section 1.18.*

20. Through the performance of the Services, EMSI collected and maintained MSI’s Confidential Information and Proprietary Information, including information concerning Transamerica’s policyholders (hereinafter referred to as “MSI’s Proprietary Information”). *See Ex. B, at Sections 1.4, 1.18 (definitions).*

21. Pursuant to Section 5.7 of the Contract, MSI’s Proprietary Information is and shall at all times remain the sole and exclusive property of MSI.

22. EMSI is obligated to protect MSI’s Proprietary Information relating to policyholders and is not permitted to disclose such data to any person. *Ex. B, Section 5.5(b). See also Ex. B to the Contract, ¶3 (setting forth EMSI’s obligation to protect MSI’s Company Information Assets); Ex. B, Sections 5.11-5.13, as amended by the business associate agreement, attached hereto as Exhibit C (hereinafter, the “BAA”) (setting forth EMSI’s obligation to safeguard protected health information).*

23. EMSI is obligated to destroy MSI’s Proprietary Information, including Confidential Information, upon request from MSI. *Ex. B, at Section 3.17 (Disposal and Destruction of Confidential Information).*

24. EMSI is required to return MSI's Proprietary Information at the request of MSI. Ex. B, Section 5.5(e) (Return of Proprietary Information).

25. MSI also has the right to examine and copy MSI's Proprietary Information and other records and practices of EMSI relating to the Services to ensure compliance with the Contract, including without limitation, all confidentiality and privacy obligations. Ex. B, Section 11.15.

26. EMSI's duties to protect, return, destroy, and provide access to Proprietary Information survive termination of the Contract. Ex. B, Section 11.12.

MSI's Demand for the Return and Destruction of the
MSI's Proprietary Information and EMSI's Asset Sale

27. Following EMSI's announcement on July 3, 2020, that it would cease operations, MSI wrote to EMSI by letter and by e-mail on multiple occasions to demand the immediate return of MSI's Proprietary Information and the subsequent destruction of the same.

28. On July 9, 2020, MSI wrote to EMSI by letter to provide notice of breach and termination of the Contract due to EMSI's failure to perform the Services and provide advance notice of its sudden closure. MSI also demanded assurances that EMSI was in compliance with its privacy and security obligations under the Contract and the BAA. Finally, MSI demanded the return of all Proprietary Information and other records no later than July 24, 2020.

29. On July 21, 2020, Jim Huyck, VP and Corporate Controller of EMSI emailed MSI to obtain payment on outstanding invoices. In response, MSI demanded a response to MSI's July 9 letter.

30. On July 22, 2020, Mr. Huyck indicated that the return of the data on its servers was not feasible because it is "spread out over multiple servers, computers, etc." Mr. Huyck stated

EMSI was in the process of destroying all physical and electronic records and would be able to provide a certificate at the conclusion of that process.

31. On July 27, 2020, MSI responded to protest EMSI's position that it could not return MSI's Proprietary Information. MSI demanded a status from EMSI on when MSI would receive records related to completed orders. MSI also notified EMSI that it intended to offset any amounts that may be due to EMSI against any costs and expenses MSI has incurred as a result of EMSI's continuing breach of the Contract.

32. On July 29, 2020, Mr. Huyck wrote to MSI by e-mail and stated that "no data had been destroyed" and indicated EMSI was "finalizing a process to address all EMSI's customer's data" and "assessing what that will take [to return the data] given the IT requirements involved." Mr. Huyck failed to address or agree to any of MSI's specific demands and indicated an "EMSI representative will be in contact regarding next steps."

33. On August 4, 2020, despite MSI's written demands pursuant to the Contract for the return of MSI's records and data, EMSI notified MSI by e-mail that it had sold its data servers to a third party, RDI Xtract, in breach of the Contract (the "Asset Sale").³ Specifically, EMSI stated:

As part of the transaction, RDI Xtract assumed control of the majority of the EMSI IT environment, including the servers and data center housing EMSI's customer data. In addition to hiring several former EMSI employees, RDI Xtract has agreed to maintain, secure and protect all data on the acquired EMSI servers and work with former EMSI customers to determine a solution for their data. ... EMSI no longer has access to the data nor the servers upon which it is stored.

34. In its August 4 e-mail, EMSI directed MSI to Kamette Myers, President of RDI Xtract, for more information about its data. Ms. Myers is a former EMSI employee. Upon

³ A true and correct copy of the August 4, 2020, e-mail from EMSI is attached hereto as Exhibit D.

information and belief, Ms. Myers worked for EMSI from June 2004 through July 2020, serving lastly as Senior Vice President of Sales and Relationship Management at EMSI. Upon information and belief, in her role at EMSI, Ms. Myers had knowledge of the Services EMSI was obligated to perform under the Contract.

35. Upon information and belief, as part of the consideration for the Asset Sale, RDI Xtract agreed to return or destroy EMSI's former customers' data upon receipt of such requests from EMSI's former clients. Upon information and belief, RDI Xtract agreed to act as EMSI's business associate (*i.e.*, subcontractor) with respect to protecting, maintaining, returning and destroying EMSI's former customer's data, including MSI's Proprietary Information.

MSI's Demands of RDI Xtract for the Return and Destruction
of the MSI's Proprietary Information

36. On August 11, 2020, MSI wrote to Ms. Myers to demand the return of all Proprietary Information and other records no later than August 18 and the subsequent destruction of the Proprietary Information no later than August 28, 2020. MSI also demanded written assurances that RDI Xtract was in compliance with the privacy and security obligations under the Contract and the BAA.

37. On August 14, 2020, MSI's counsel wrote to EMSI to inform it that RDI Xtract had not yet agreed to return MSI's Proprietary Information and to renew its demands for the return of all MSI Proprietary Information. MSI again demanded assurances that EMSI was in compliance with its privacy and security obligations under the Contract and the BAA. MSI also demanded, if necessary, EMSI make available its resources to RDI Xtract to comply with MSI's demands. And MSI again notified EMSI of its intent to offset any amounts that may still be due to EMSI against

any costs and expenses MSI has incurred as a result of EMSI's continuing breach of the Contract. EMSI did not respond to this letter.

38. On August 14, 2020, Ms. Myers responded by e-mail to MSI's letter and reported that she was "continuing to work through this document and am pushing forward with our necessary steps to return the data required by August 28." Ms. Myers also requested a telephone conference.

39. On August 17, 2020, MSI spoke with Ms. Myers, President of RDI Xtract, and RDI Xtract's outside general counsel, Mike Coles. Ms. Myers confirmed that RDI Xtract had purchased certain of EMSI's assets, including data servers and other equipment. Ms. Myers confirmed that MSI's Proprietary Information is stored on the acquired data servers. Ms. Myers also informed MSI that RDI Xtract did not have the IT resources necessary to assist MSI in any effort to return the servers storing the MSI Proprietary Information. Ms. Myers indicated that MSI would need to engage RDI Xtract to perform any services related to the return of the MSI Proprietary Information, and that RDI Xtract would need to hire a former EMSI employee to perform that work.

40. During the August 17, 2020, telephone call, Ms. Myers and Mr. Coles also informed MSI that RDI Xtract did not have physical or electronic access to the servers. According to Ms. Myers and Mr. Coles, EMSI remains in possession and control over the servers. Therefore, according to Ms. Myers and Mr. Coles, RDI Xtract could not comply with MSI's demands until such time that RDI Xtract obtains control over the servers. Ms. Myers and Mr. Coles stated that RDI Xtract may gain access around the end of August.

41. Upon information and belief, RDI Xtract has electronic access to the servers, as well as the ability to physically access the servers upon request, and RDI Xtract's statements to

the contrary were intended to cause MSI to delay its efforts to safeguard and retain control over MSI's Proprietary Information.

42. Upon information and belief, RDI Xtract is in the process of assuming the lease for EMSI's headquarters.

43. Upon information and belief, RDI Xtract nonetheless has physical and electronic access to the servers storing the MSI's Proprietary Information.

44. Upon information and belief, EMSI also retains access to the servers storing the MSI's Proprietary Information in connection with its efforts to wind down its business.

45. RDI has not committed to the return of MSI's Proprietary Information and, as of August 17, claimed not to have the access or resources necessary to effect the return of MSI's Proprietary Information.

46. On August 25, 2020, counsel for MSI wrote to RDI Xtract by e-mail to demand the return of MSI's Proprietary Information, destruction of the data following its safe return to MSI, and provide a certificate of destruction. MSI also demanded access to the Irving, TX facility to examine the records and audit EMSI's and RDI's compliance with its privacy and security obligations. As of end of business on August 27, 2020, RDI had not responded to MSI's demands.

47. EMSI has also not agreed to return MSI's Proprietary Information, destroy the data following its safe return, and provide a certificate of destruction. Further, since August 4, 2020, EMSI maintains it does not have control over the MSI Proprietary Information and continues to direct MSI to RDI Xtract for the return and subsequent destruction of the same.

48. At this time, RDI and EMSI each claim not to have control over the servers that house MSI's Proprietary Information.

49. The safe return and retention of MSI's Proprietary Information is critical to MSI's business.

CAUSES OF ACTION

FIRST CAUSE OF ACTION (AS AGAINST RDI): TORTIOUS INTERFERENCE WITH AN EXISTING CONTRACTUAL RELATIONSHIP

50. MSI incorporates by reference the preceding paragraphs as if fully set forth herein.

51. MSI has a contractual relationship with EMSI pursuant to which EMSI was obligated to protect MSI's Proprietary Information and to return and destroy such data upon request from MSI. Ex. B, Section 3.17 (Disposal and Destruction of Proprietary Information); Section 5.5(e) (Return of Proprietary Information); and Sections 5.5, 5.11-5.13, as amended by the BAA.

52. By relinquishing control over MSI's Proprietary Information in connection with the Asset Sale and subsequently refusing to return and destroy MSI's Proprietary Information following MSI's demands, EMSI has repudiated its obligations in breach of the Contract.

53. Upon information and belief, RDI knew that EMSI was obligated to hold its customers' data and information in confidence and return or destroy its customers' data following any termination of the Contract or upon request. Indeed, upon information and belief, RDI agreed to perform those duties and act as EMSI's business associate in that regard.

54. Further, upon information and belief, RDI knew that EMSI's customers, including MSI, had requested the return or destruction of their data and that EMSI was obligated to comply with those requests.

55. Upon information and belief, RDI willfully and intentionally induced or otherwise conspired with EMSI to sell MSI's Proprietary Information or otherwise transfer possession and control of such data to RDI Xtract, despite knowing the transaction would prevent EMSI from protecting the data and from returning and destroying the data, as EMSI was obligated to do under the Contract.

56. RDI's efforts to induce EMSI, a distressed corporation in the process of winding down its business, to breach the Contract caused MSI immediate and irreparable harm. MSI has and will continue to incur actual damages as a direct result of RDI's interference with the Contract, including but not limited to damages associated with its investigation and securing substitute services with no advance notice to secure the return of and protections for MSI's Proprietary Information.

**SECOND CAUSE OF ACTION (AS AGAINST EMSI):
BREACH OF CONTRACT**

57. MSI incorporates by reference the preceding paragraphs as if fully set forth herein.

58. Under the Contract, EMSI was obligated to perform the Services and breached the Contract by ceasing operations without providing advance notice to MSI, as required.

59. Under the Contract, EMSI agreed to protect MSI's Proprietary Information from unauthorized access and to ensure that such data was not disclosed or otherwise made available to a third party. *See, e.g.*, Sections 5.5, 5.11-5.13, as amended by the BAA.

60. Under Section 5.5(e) of the Contract, EMSI agreed to return MSI's Proprietary Information upon request. MSI requested the return of the MSI's Proprietary Information on July 9, 27 and August 14, 2020.

61. Under Sections 3.17 and 5.12 of the Contract, as amended, EMSI further agreed to destroy MSI's Proprietary Information upon request.

62. EMSI's duties to protect, return, and destroy MSI's Proprietary Information survive termination of the Contract. Ex. B, Section 11.12.

63. EMSI's duties to safeguard, return and destroy all MSI Proprietary Information are integral components of the Services. *See* Section 3.9 (providing each Statement of Work is deemed to incorporate the terms and conditions of the Contract by reference).

64. MSI's Proprietary Information is the sole and exclusive property of MSI. *See* Ex. B, Section 5.7. Any assignment or transfer or attempt to assign or transfer any of rights under the Contract without MSI's written consent is void under the Contract. *See* Ex. B, Section 11.1.

65. By relinquishing control over MSI's Proprietary Information in connection with the Asset Sale and subsequently refusing to return and destroy MSI's Proprietary Information following MSI's repeated demands, EMSI has repudiated its obligations to protect, return, and destroy MSI's Proprietary Information in breach of the Contract.

66. MSI has incurred and continues to incur damages resulting from EMSI's breach of the Contract and is entitled to recover any and all such damages. In addition, because MSI's Proprietary Information is unique and critical to MSI's ongoing business, MSI is entitled to an order of specific performance requiring EMSI to immediately provide MSI with MSI's Proprietary Information.

**THIRD CAUSE OF ACTION (AS AGAINST RDI AND EMSI):
APPLICATION FOR TEMPORARY RESTRAINING ORDER, TEMPORARY
INJUNCTION, AND PERMANENT INJUNCTION**

67. MSI incorporates by reference the preceding paragraphs as if fully set forth herein.

68. A temporary restraining order, and a subsequent temporary injunction, is necessary because (i) MSI owns MSI's Proprietary Data and is entitled to the safe return and destruction of the same, (ii) RDI has no right to access or disclose MSI's Proprietary Data, for any purpose, (iii) MSI is obligated under the law to protect its Proprietary Information from unauthorized disclosure, (iv) MSI can establish a probable right to the relief sought, and (v) MSI can establish a probable, imminent, and irreparable harm in the interim.

69. As alleged in the paragraphs above, MSI has valid causes of action and is likely to prevail against EMSI for breach of contract and RDI for tortious interference with an existing contract.

70. At this time, RDI and EMSI each claim not to have control over the servers that house MSI's Proprietary Information. Further, RDI represented it has only limited IT resources and would be unable to access and retrieve the data without hiring additional IT resources. Further, MSI requested and RDI has not provided written assurances that it is in compliance with its privacy and security obligations. The proper safeguarding, preservation and return of MSI's Proprietary Information is critical to its business. MSI faces immediate and direct damage and irreparable harm if any third parties gain access to the MSI's Proprietary Information.

71. MSI has no adequate remedy at law.

72. MSI requests the Court enter a temporary restraining order ex parte. As discussed above, MSI will suffer irreparable injury if the temporary restraining order is not granted. Further, because any disclosure of MSI's Proprietary Information, including customer information, would result in immediate and irreparable harm, there is inadequate time to serve notice and hold a contested hearing. Providing notice to EMSI and RDI and the delay attendant to setting a hearing

or issuing a temporary restraining order could further harm MSI by resulting in self-help remedies or other actions to deprive MSI of possession of, or access to, MSI's Proprietary Information.

73. Consequently, the need for a temporary restraining order is immediate and, if not granted, MSI will suffer irreparable harm.

74. MSI will post a bond for the temporary restraining order in the amount set by the Court. MSI requests that, because it is seeking to secure its data, the amount of any bond should be minimal.

75. MSI seeks a temporary restraining order, and a subsequent temporary injunction, that restrains or enjoins EMSI and RDI, their agents, employees, and representatives, and all persons acting on their behalf from taking any of the following actions until this dispute is resolved:

- a. Failing to protect and preserve MSI's Proprietary Information;
- b. Accessing, or allowing any other third party, to access or otherwise take physical possession of any data servers prior to the return and subsequent destruction of MSI's Proprietary Information, without MSI's advance, written consent;
- c. Denying, interfering or otherwise refusing to cooperate with MSI's rights under the Contract with respect to MSI's Proprietary Information, including its right to audit and access its data or any other documents or information to which it is entitled, including the servers on which that data is stored.

76. Further, because both RDI and EMSI are obligated to return or destroy MSI's Proprietary Information, the Court should order EMSI and RDI jointly and severally to (i) immediately return MSI's Proprietary Information in a format acceptable to MSI; (ii) securely destroy MSI's Proprietary Information and provide an affidavit attesting to the same; (iii) provide or otherwise arrange for MSI to have full and complete access to the servers that contain MSI's Proprietary Information, subject to the existing confidentiality agreements between and among the Parties, for the purpose of auditing EMSI's and RDI's privacy obligations under the Contract and

the law and to ensure the data's safe destruction pursuant to the Court's order; and (iv) provide a copy of the asset sale agreement and any related agreements between RDI and EMSI, which upon information and belief requires RDI Xtract to provide the relief requested herein. Finally, the Court should order RDI and EMSI to cooperate with any such audit and provide reasonable assistance to MSI in connection with accessing the servers for the purpose of auditing EMSI's privacy obligations and to ensure the data's safe return and destruction pursuant to the Court's order.

FOURTH CAUSE OF ACTION (AS AGAINST EMSI): ATTORNEY'S FEES

77. MSI incorporates by reference the preceding paragraphs as if fully set forth herein.

78. As a result of EMSI's breach of contract and wrongful acts and omissions, MSI retained the undersigned attorneys to represent it and agreed to pay their reasonable and necessary fees. MSI seeks recovery of its reasonable and necessary attorney's fees, court costs, and expenses through trial and all appeals under Tex. Civ. Prac. & Rem. Code § 38.001-38.003, and as otherwise authorized by law and the Contract.

MISCELLANEOUS

79. All conditions precedent to the filing of MSI's claims in this action have been performed, have already occurred, or have otherwise been met, waived, or satisfied.

80. By filing these claims, MSI does not waive or release any rights, claims, causes of action, or defenses, or make any election of remedies, and expressly reserves all such rights, claims, causes of action, or defenses, whether or not the same have been asserted or may hereafter be asserted in this or any other proceeding.

DISCOVERY REQUESTS

81. Pursuant to Texas Rule of Civil Procedure 194, RDI and EMSI is requested to disclose, within 50 days after service of this request, the information or material described in Rule 194.2.

RELIEF REQUESTED

MSI requests the following relief:

- a. that RDI and EMSI be served with process and required to answer in the time and manner prescribed by law
- b. that the Court enter a temporary restraining order, temporary injunction, and a permanent injunction, as requested above;
- c. that the Court enter an award judgment against RDI and EMSI for MSI's actual damages;
- d. that MSI recover its attorney's fees, court costs, and expenses (including, but not limited to, expert witness fees and expenses) incurred through the trial of this cause and any appeal;
- e. that MSI recover pre- and post-judgment interest at the highest rate and to the maximum extent permitted by law; and
- f. all other relief to which MSI is entitled, at law or in equity.

Respectfully submitted,

/s/ Susan Egeland

Susan Egeland

State Bar No. 24040854

susan.egeland@faegredrinker.com

FAEGRE DRINKER BIDDLE & REATH LLP

1717 Main Street, Suite 5400

Dallas, TX 75201

Telephone: (469) 357-2500

Facsimile: (469) 327-0860

ATTORNEY FOR MONEY SERVICES, INC.

LOCAL RULE 1.06 AND 2.02 CERTIFICATIONS

Pursuant to Local Rule 1.06, the undersigned counsel informs the Court that there exists a related case filed on July 27, 2020 titled *The Savings Bank Mutual Life Insurance Company of Massachusetts v. Examination Management Services, Inc. and EMSI Holding Company*, In the 68th District Court of Dallas County, Texas, Cause No. DC-20-10143. MSI advises the Court that transfer of this case to the 68th District Court “would facilitate orderly and efficient disposition of the litigation” as contemplated by Local Rule 1.06.

Pursuant to Local Rule 2.02, the undersigned counsel certifies they will send Defendants, through the EMSI Board (Board@emsinet.com), Troy Phillips, a member of the EMSI Board (tphillips@bpoc.com), Kamette Myers, President of RDI Xtract (kmyers@rdixtract.com), and Mike Coles (mikec@colesfirm.com), counsel for RDI Xtract and RDI Corporation, a copy of this Petition and the proposed Temporary Restraining Order at least 2 hours before the application and proposed order are to be presented to the Court for decision

/s/ Susan Egeland
Susan Egeland

DC-20-12059

CAUSE NO. _____

MONEY SERVICES, INC.

Plaintiff,

v.

**EXAMINATION MANAGEMENT
SERVICES, INC., EMSI HOLDING
COMPANY, RDI XTRACT, LLC, RDI
CORPORATION**

Defendants.

§ IN THE DISTRICT COURT OF

**§
§ DALLAS COUNTY, TEXAS
§**

**§
§ JUDICIAL DISTRICT COURT
§
§**

TEMPORARY RESTRAINING ORDER

After considering Plaintiff's Original Petition, Application for Temporary Restraining Order, and Application for Temporary and Permanent Injunctive Relief, and the pleadings, declarations, and arguments of counsel, the Court finds and concludes that there is sufficient evidence that, if it does not enter this Temporary Restraining Order, there is a serious and imminent threat that Plaintiff Money Services, Inc. ("MSI") will suffer irreparable harm from the actions of Examination Management Services, Inc., EMSI Holding Company, RDI Xtract LLC ("RDI Xtract") and RDI Corporation (collectively, "Defendants") with respect to the business information of MSI. Specifically, the verified allegations of MSI establish that (1) EMSI transferred control of data servers that store records created and maintained by Examination Management Services, Inc. (EMSI) on behalf of MSI, including MSI's Proprietary Information, to RDI Xtract without MSI's authorization; (2) MSI is the exclusive owner of its Proprietary Information; (3) EMSI and RDI Xtract have refused to return and subsequently destroy MSI's Proprietary Information, which RDI Xtract and EMSI are obligated to do upon request; (4) MSI faces immediate and direct damage and irreparable harm with regard to its business if its

Proprietary Information is not safely returned or if any third parties gain access to its Proprietary Information.

The Court has been advised that at least two hours' notice of this application for a Temporary Restraining Order has been provided to Defendants. The Court finds that an ex parte order and hearing without further notice to Defendants is warranted because it appears that MSI may have already suffered irreparable injury, loss, or damage and that there is a threat of continuing irreparable harm, loss, or damage to MSI if a restraining order is not granted as requested, to wit, the risk of unauthorized disclosure of MSI's records to RDI Xtract or other third parties and permanent loss of MSI's Proprietary Information, which is important for MSI's ongoing business operations.

Accordingly, the Court hereby orders that Defendants, their directors, officers, employees, agents, representatives, and counsel, and all other persons and entities in active concert or participation with any of them, are and shall be enjoined and restrained from:

- a. Failing to protect and preserve MSI's Proprietary Information;
- b. Accessing, or allowing any other third party, to access or otherwise take physical possession of any data servers prior to the destruction of MSI's Proprietary Information, without MSI's advance, written consent;
- c. Denying, interfering or otherwise refusing to cooperate with MSI's rights under the Contract with respect to MSI's Proprietary Information, including its right to audit and access its data or any other documents or information to which it is entitled, including the servers on which that data is stored.

The Court further orders Defendants jointly and severally to (i) immediately return MSI's Proprietary Information on behalf of EMSI in a format acceptable to MSI; (ii) securely destroy MSI's Proprietary Information on behalf of EMSI and provide an affidavit attesting to the same; (iii) provide or otherwise arrange for MSI to have full and complete access to the servers that contain MSI's Proprietary Information, subject to the Parties' existing confidentiality agreements,

for the purpose of auditing RDI's and EMSI's privacy obligations under the Contract and the law and to ensure the data's safe destruction pursuant to the Court's order; and (iv) provide a copy of the asset sale agreement and any other agreements related to the sale of the data servers. The Court further orders Defendants to cooperate and provide reasonable assistance to MSI in connection with accessing the servers for the purpose of auditing RDI's and EMSI's privacy obligations and to ensure the data's safe return and destruction pursuant to the Court's order.

The Court sets bond in the amount of \$_____.

Unless it is extended in writing before _____, 2020, by further written order of this Court, this Temporary Restraining Order expires on its own terms at _____ on August, 2020.

IT IS SO ORDERED.

SIGNED at _____ .m. on this _____ day of August, 2020.

JUDGE PRESIDING

Exhibit A

CAUSE NO. _____

MONEY SERVICES, INC.

Plaintiff,

V.

**EXAMINATION MANAGEMENT
SERVICES, INC., EMSI HOLDING
COMPANY, RDI XTRACT, LLC, RDI
CORPORATION**

Defendants.

IN THE DISTRICT COURT OF

DALLAS COUNTY, TEXAS

JUDICIAL DISTRICT COURT

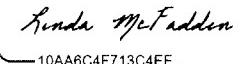
**DECLARATION (IN LIEU OF AFFIDAVIT) IN SUPPORT OF
PLAINTIFF'S ORIGINAL PETITION, APPLICATION FOR TEMPORARY
RESTRANING ORDER, AND APPLICATION FOR TEMPORARY AND
PERMANENT INJUNCTIVE RELIEF**

I, Linda McFadden, declare and state as follows, in accordance with Texas Civil Practice and Remedies Code Section 132.001(a):

"I am over the age of 18 (DOB 08/03/1969), have never been convicted of a felony or crime involving moral turpitude and am duly qualified and competent to execute this affidavit and the facts contained herein are true and correct based upon the knowledge I obtained from review of the materials pertaining to this matter. Money Services, Inc. provides services to its affiliated companies and divisions of such companies, including Transamerica Life Insurance Company. My name is Linda McFadden. My office address is Transamerica, located at 6600 Chase Oaks Blvd, Ste. 140, Plano, TX 75023, and I am a Lead Vendor Manager at Transamerica.

I have read the attached Plaintiff's Original Petition, Application for Temporary Restraining Order, and Application for Temporary and Permanent Injunctive Relief and the facts stated therein are true and correct to the best of my current knowledge."

Executed in Frisco, Texas on August 27, 2020.

DocuSigned by:

10AA6C4F713C4EF...
Linda McFadden

CAUSE NO. _____

MONEY SERVICES, INC.

Plaintiff,

v.

EXAMINATION MANAGEMENT
SERVICES, INC., EMSI HOLDING
COMPANY, RDI XTRACT, LLC, RDI
CORPORATION

Defendants.

§ IN THE DISTRICT COURT OF

§ DALLAS COUNTY, TEXAS

§ JUDICIAL DISTRICT COURT

§

**DECLARATION (IN LIEU OF AFFIDAVIT) IN SUPPORT OF
PLAINTIFF'S ORIGINAL PETITION, APPLICATION FOR TEMPORARY
RESTRAINING ORDER, AND APPLICATION FOR TEMPORARY AND
PERMANENT INJUNCTIVE RELIEF**

STATE OF TEXAS §

§

COUNTY OF TARRANT §

I, Susan Egeland, declare and state as follows, in accordance with Texas Civil Practice and Remedies Code Section 132.001(a):

"I am over the age of 18 (DOB 8/9/78), have never been convicted of a felony or crime involving moral turpitude and am duly qualified and competent to execute this affidavit and the facts contained herein are true and correct based upon the knowledge I obtained during the course of my representation of Money Services, Inc. in this matter and my review of the materials pertaining to the same. My name is Susan Elizabeth Egeland. My office address is Faegre Drinker Biddle & Reath LLP, located at 1717 Main Street, Suite 5400, Dallas, Texas 75201, and I am one of the attorneys representing Plaintiff Money Services, Inc. in this lawsuit.

I have read the attached Plaintiff's Original Petition, Application for Temporary Restraining Order, and Application for Temporary and Permanent Injunctive Relief and the facts stated therein are true and correct to the best of my current knowledge."

Executed in Tarrant County, State of Texas on August 28, 2020.



Susan Elizabeth Egeland
Counsel for Plaintiff

Exhibit B

**MONEY SERVICES, INC.
PROFESSIONAL SERVICES AGREEMENT**

This Professional Services Agreement ("Agreement") is entered into as of the 1ST day of April, 2014 (the "Effective Date"), by and between Money Services, Inc. ("Company") located at 4333 Edgewood Road, Cedar Rapids, Iowa 52499 and Examination Management Services, Inc. ("Service Provider") located at 3050 Regent Boulevard, Suite 400, Irving, Texas 75063.

WHEREAS, Company desires to retain Service Provider to provide Services related to the Services defined in Exhibit C and Exhibit D herein for Company Affiliates, and Service Provider is willing to provide such Services subject to the terms of this Agreement;

WHEREAS, Company possesses certain confidential and/or proprietary information and in connection with the Services, Company confidential and/or proprietary information will become available or disclosed to, or will be generated by, Service Provider, and Company desires to prevent the unauthorized use and disclosure of such confidential and/or proprietary information;

WHEREAS, in addition to the Services contemplated by the parties, Service Provider may also provide information technology services or other Deliverables related to the provision of Services;

WHEREAS, privacy requirements have been enacted into law pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as well as other state and federal laws, which requirements impose on Company the obligation to enter into a Business Associate Agreement for some of the Services; and

WHEREAS, as a result of the Services and access to confidential and/or proprietary information, Service Provider may design, create, invent or initiate further proprietary information and Company and Service Provider desire that such proprietary information shall belong to Company.

NOW, THEREFORE, in consideration of the covenants set forth herein, and for other good and valuable consideration, the receipt, adequacy and sufficiency of which is hereby acknowledged, the parties agree as follows:

1. **DEFINITIONS.** The following terms have the meanings ascribed to them when used in this Agreement or in any Statement of Work. Other terms, when capitalized, have the meanings defined elsewhere in this Agreement.

1.1 An "**Affiliate**" of a specified Person is a Person that directly or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with, the Person specified. For the purpose of this definition, the term "control" (including the terms "controlling," "controlled by" and "under common control with") means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a Person, whether through the ownership of voting securities, by contract, or otherwise.

1.2 "**Applicable Laws**" means all applicable conventions, laws, rules, regulations and orders of governmental authorities having jurisdiction over the subject matters of this Agreement, including without limitation, state and federal anti-kickback and anti-referral laws and regulations.

1.3 "**Change Order**" is defined in Section 3.10.

1.4 "**Confidential Information**" shall mean information identified on, in or constituting: all strategic and development plans, financial information, results of the Services, business plans, information about the Disclosing Party and/or its Affiliates, co-developer identities, data, business records, customer lists, policy information, personally identifiable information, personal financial information or personal health information (as those terms are defined by governing law), product designs, test data, project records, market reports, investor information, know-how, discoveries, ideas, concepts, specifications, models, diagrams, methodologies, research, technical and statistical data, drawings, models, flow charts, work-flow, marketing, pricing, selling, distribution, database descriptions, software code, source code, object code, Intellectual Property, and any and all other tangible or intangible information, other than Trade Secrets, encompassed in any medium, which may be disclosed, whether or not in writing, whether or not marked as "Confidential" or "Proprietary" by the Disclosing Party or to which the

Receiving Party may be provided access to by Disclosing Party in accordance with this Agreement, or which is generated or learned as a result of or in connection with the Services and is not generally available to the public. "Confidential Information" also includes proprietary or confidential information of any third party that may disclose such information to either party in the course of the third party's relationship with such party. For clarification purposes, Confidential Information includes Nonpublic Personal Financial Information, Protected Health Information, and Electronic Protected Health Information.

1.5 **Cure Period** is defined in Section 7.2.

1.6 **Deliverables** means the Services and tangible items that are specified in and provided to Company pursuant to a Statement of Work issued under this Agreement and includes, without limitation, any materials, documentation, designs, drawings, data files, computer programs, textual items, audio and visual items, graphical items and modifications thereto (including both source code and object code) and other works of authorship resulting from the performance of Services under this Agreement by Service Provider, its agents and subcontractors, whether fixed in digital, magnetic or optical media or document form.

1.7 **DHHS** means the United States' Department of Health and Human Services.

1.8 **Disclosing Party** is defined in Section 5.5.

1.9 **Electronic Protected Health Information** or "**ePHI**" means any information that: (A) relates to the past, present, or future physical or mental health or condition of a Policyholder, the provision of health care to a Policyholder, or the past, present or future payment for the provision of health care to a Policyholder; (B) that identifies a Policyholder, or with respect to which there is a reasonable basis to believe the information can be used to identify the Policyholder; and (C) that is transmitted by electronic media or maintained in electronic media and as further defined within 45 CFR 160.103 (as amended or superseded from time to time).

1.10 **Force Majeure** means any act or event, whether foreseen or unforeseen, that meets all three of the following:

- (a) The act or event prevents the nonperforming party, in whole or in part, from:
 - (i) performing its obligations under this Agreement; or
 - (ii) satisfying any conditions to the performing party's obligations under this Agreement.
- (b) The act or event is beyond the reasonable control of and not the fault of the nonperforming party.
- (c) The nonperforming party has been unable to avoid or overcome the act or event by the exercise of due diligence;

provided, however, that, notwithstanding (a), (b) and (c) above and in any event, Force Majeure excludes economic hardship, labor strikes or shortages, changes in market conditions or insufficiency of funds.

1.11 **HIPAA Covered Products** means any insurance products offered by Company or any of its Affiliates which are subject to HIPAA and/or HITECH, as amended from time to time.

1.12 **Implementation Schedule** means a schedule set forth in a Statement of Work for the delivery or implementation of one or more Deliverables to which the Statement of Work pertains, listing "milestones" based on key occurrences, such as the development of Specifications, delivery of items for testing, completion of tests and the like.

1.13 **Intellectual Property** means any and all now known or hereafter known or developed tangible and intangible: (a) rights associated with works of authorship throughout the universe, including, but not limited to, copyrights, moral rights and mask works; (b) trademarks, services marks, trade names and any other indicia of origin; (c) Trade Secrets; (d) patents, pending patent applications, designs, algorithms and other industrial property rights; (e) all other intellectual and industrial property rights (of every kind and nature throughout the universe and however designated, including "rental" rights and rights to remuneration), whether arising by operation of law, contract, license or otherwise; and (f) all registrations, initial applications, renewals, extensions, continuations, divisions or reissues now or hereafter in force (including any rights in any of the foregoing).

1.14 **“Nonpublic Personal Financial Information”** means personally identifiable financial information about Policyholders and includes, without limitation, any list, description, or other grouping of Policyholders (and publicly available information pertaining to them) that is derived using any nonpublic personal information; provided, however, that the above definition shall be superseded and replaced to the extent that the definition of Nonpublic Personal Financial Information under Title V of Public Law 106-102, Section 509, subsection (4) (as amended or superseded from time to time) differs therefrom.

1.15 **“Person”** shall be construed as broadly as possible and shall include, without limitation, any natural person, corporation, partnership, limited partnership, limited liability company, trust, group, association or other entity.

1.16 **“Policyholder”** means any individual or entity who presently or in the past has applied for, owned or been covered by a product offered by Company or its Affiliates.

1.17 **“Policy”** and **“Policies”** means insurance policies or certificates of insurance coverage issued by Company or its Affiliates.

1.18 **“Proprietary Information”** means Confidential Information and Trade Secrets, whether in written, oral, electronic or other form, furnished, transmitted to, observed or obtained by one of the parties (including, without limitation, any Confidential Information or Trade Secrets that are in a party’s facility and are viewable, accessible or otherwise made available to Receiving Party); provided, however, that, to the extent reasonably substantiated by documentation, the following information is not Proprietary Information and Receiving Party is not restricted as to its use or disclosure:

- (a) information already in the possession of, or already known to, the Receiving Party as of the Effective Date, and not under any other obligations of confidentiality due to any other agreements between the parties;
- (b) information that enters the public domain after the Effective Date, or which, after such disclosure, enters the public domain through no fault of the Receiving Party;
- (c) information lawfully furnished or disclosed to the Receiving Party by a non-party to this Agreement without any obligation of confidentiality;
- (d) information independently developed by any party without use of any Proprietary or Confidential Information; or
- (e) information that is explicitly approved for release by the Disclosing Party.

1.19 **“Protected Health Information”** or **“PHI”** shall have the same meaning as the term “protected health information” in 45 C.F.R. §164.501 (as amended or superseded from time to time), limited to information created or received by Service Provider or its affiliates from or on behalf of Company and its Affiliates, or otherwise created or received by Service Provider, and shall include, without limitation, any and all information that relates to the past, present, or future physical or mental health or condition of a Policyholder, to the provision of health care to a Policyholder, or to the past, present, or future payment for the provision of health care to a Policyholder, and that identifies Policyholder or for which there is a reasonable basis to believe that the information can be used to identify the Policyholder, in each case regardless of whether the Policyholder is living or deceased. By way of illustration only, the following information shall constitute Protected Health Information with respect to a Policyholder: (i) name, (ii) street address, city, county, precinct, and zip code, (iii) dates directly related to the Policyholder, including birth date, (iv) telephone numbers, fax numbers, and electronic mail addresses, (v) social security number, (vi) policy or certificate number, and (vii) any other unique identifying numbers, characteristics, or codes. Such information shall constitute Protected Health Information regardless of whether it is in electronic, paper, or any other format.

1.20 **“Receiving Party”** is defined in Section 5.5.

1.21 **“Representative”** means any director, officer, employee, agent, representative, advisor or consultant of either of the parties or any director, officer, employee, agent, representative, advisor or consultant of an Affiliate. The term “Representative,” when used with respect to Service Provider, shall include such Subcontractors and their respective directors, officers, employees, agents, representatives, advisors and consultants.

1.22 **"Self-Help Code"** means any back door, time bomb, trap door, drop dead device, or other software routine designed to disable a computer program automatically with the passage of time or under the positive control of a person other than a user of the program. Self-Help Code does not include software routines in a computer program, if any, designed to permit an owner of the computer program (or other person acting by authority of the owner) to obtain access to a user's computer system(s) (e.g., remote access via modem) for purposes of maintenance or technical, or other purposes indicated in the applicable software's documentation.

1.23 **"Services"** mean all Services to be furnished to Company by Service Provider or its subcontractors as set forth in an applicable Statement of Work.

1.24 **"Specifications"** mean the functional and operating specifications and requirements of any Deliverable, as set forth in an applicable Statement of Work.

1.25 **"Statement of Work"** means a written instrument that meets the requirements of Section 3, and is executed by the authorized representatives of both parties for the performance of Services or the creation of Deliverables and which shall, once executed, form an integral part of this Agreement.

1.26 **"Term"** is defined in Section 9.1.

1.27 **"Trade Secrets"** mean technical and non-technical information (regardless of whether such information is in tangible or intangible form) including source code, object code, computer code, data, ideas, concepts, formulae, methods, techniques, processes, financial business plans and business methods (including any derivatives of any of the foregoing) disclosed to either party by or on behalf of the other party that derive economic value, actual or potential, from not being generally known to other persons who could obtain economic value from the disclosure or use thereof, and which are the subject of efforts that are reasonable under the circumstances to maintain their secrecy.

1.28 **"Unauthorized Code"** means any virus, salamis, Trojan horse, Easter eggs, logic bomb, worm, programs or computer instructions that self-replicate without manual intervention, or other software routines or hardware components designed to permit unauthorized access, disable, erase, or otherwise harm software, hardware, or data, or to perform any other unauthorized actions. The term Unauthorized Code does not include Self-Help Code.

1.29 **"Virus"** means any computer instructions designed to disrupt, disable, harm, alter, destroy or otherwise impede in any manner, including aesthetical disruptions or distortions, the operation of the Software, or any other software, data storage, computer libraries, firmware, hardware or computer system (including local area or wide-area networks). Viruses include, but are not limited to, Self-Help Code and Unauthorized Code.

2. **RELATIONSHIP OF PARTIES.**

2.1 **Independent Contractor.**

(a) **Service Provider as Independent Contractor.** Service Provider agrees and acknowledges that Service Provider is an independent contractor under this Agreement, with the authority to control the manner, method and means of Service Provider's performance. Company shall inform Service Provider only of the results it desires, the completion date, and assessment of the Services to ensure they have been performed in accordance with Service Provider's engagement. Personnel supplied by Service Provider hereunder are not employees or agents or Company or its Affiliates and Service Provider assumes full responsibilities for their acts. Nothing contained in this Agreement shall be deemed or construed to create an employer/employee relationship or any partnership or joint venture between Service Provider and Company. Service Provider acknowledges and agrees that only eligible employees of Company are entitled to benefits under Company (i) pension and welfare plans (as the Employment Retirement Income Security Act defines those terms) and (ii) any other benefit arrangements, and that Service Provider's status as an independent contractor makes Service Provider ineligible to participate in these plans and arrangements. Service Provider shall not at any time hold itself out as an employee of Company. The parties shall not make any commitments or incur any charges or expenses for or in the name of one another and shall, to the greatest extent possible, perform this Agreement in a manner consistent with Service Provider's status as an independent contractor.

(b) Subcontractors. Service Provider may subcontract with another person or entity (each a "Subcontractor") for the performance of some or all the Services; provided, however, that no subcontract shall relieve Service Provider from any obligations or liabilities hereunder and Service Provider shall remain responsible for all obligations or liabilities of each Subcontractor with respect to provision the Services as if provided by Service Provider. Service Provider shall cause each Subcontractor and its employees, agents, and representatives to comply with the terms and conditions of this Agreement applicable to them. Service Provider shall, at the request of Company in its sole reasonable discretion, cease using any Subcontractor to Service the Company or its Affiliates.

2.2 **Administration of Contract.**

(a) Personnel.

(i) Qualifications. Service Provider shall provide individuals who are duly qualified and skilled in the area in which their Services are to be utilized ("Placed Personnel"). Company possesses the right to reasonably reject any individual so furnished, if dissatisfied with such individual's performance. If any Placed Personnel is rejected, Service Provider agrees to use commercially reasonable efforts to furnish a suitable replacement within a reasonable time.

(ii) Reassignment. Service Provider shall use commercially reasonable efforts to adhere to applicable staffing plans to meet forecasted support requests. If any personnel change occurs, Service Provider shall adhere to schedules, absorb costs of any unavoidable duplication or retraining, and assure that personnel of at least comparable qualifications and experience are assigned to complete the Services and are reasonably satisfactory to Company.

(iii) Drug and Background Screens. Service Provider agrees to notify its Placed Personnel who perform Services under this Agreement of the Service Provider's policy concerning drug and alcohol use that prohibits (A) the use, possession, distribution, purchase or sale of drugs or alcohol on Company's premises or while engaged in Service Provider's business and (B) reporting to or performing work for Company while under the influence of drugs or alcohol (except for authorized amounts of over-the-counter or prescribed drugs required for health reasons). Further, Service Provider agrees that its policy will allow Service Provider:

- a. to screen any Placed Personnel for the unauthorized or unlawful use of drugs by having Placed Personnel submit to a licensed laboratory for screening or be terminated. Service Provider further agrees to confirm that any Placed Personnel did not engage in the unauthorized or unlawful use of drugs at the time of such screen. If Service Provider cannot confirm such, Service Provider shall promptly remove such Placed Personnel and replace him or her with replacement personnel with substantially the equivalent or better qualifications within seven (7) days.
- b. to conduct a background investigation that will confirm that the Placed Personnel has not been convicted of a felony involving theft, dishonesty, or breach of trust, or any provision of the Federal Crime Bill. If Service Provider cannot confirm such within thirty (30) days of placement of the Placed Personnel, Service Provider shall immediately remove Placed Personnel and replace him or her with replacement personnel with substantially the equivalent or better qualifications within seven (7) days.

(iv) Compliance with Laws. Service Provider represents and warrants that in the course of providing Services under this Agreement that Service Provider shall comply with all applicable federal, state and local laws, rules, regulations, ordinances, codes, orders and/or programs. Service Provider further represents and warrants that it will have obtained any necessary permits, licenses or any other documentation and authorization required to comply with any such laws and regulations. Service Provider hereby certifies that it shall fully comply with Executive Order 11246, as amended by Executive Order 11375, Section 503 of the Rehabilitation Act of 1973, as amended, the Vietnam War Veteran Readjustment Assistance Act of 1974, as amended, Executive Order 11625, as amended and the rules and regulations issued thereunder, any privacy laws, the Fair Labor Standards Act, the Equal Pay Act, the Occupational Safety and Health Act, Americans with Disabilities Act, The Age Discrimination in Employment Act, Title VII of the Civil Rights Act, Immigration and Control Act,

Family and Medical Leave Act, and provisions relating to the identification and procurement of required permits, certificates, approvals and inspections, labor and employment obligations, affirmative action, and wage and hour laws, which are hereby incorporated by reference as appropriate. Service Provider commits itself to such compliance by entering into this Agreement. Service Provider shall require its applicable subcontractors to comply with this Section.

(b) **Access to Premises.** Company agrees to provide Service Provider with physical access to premises under the control of Company as may be necessary for Service Provider to perform its obligations under this Agreement. Company agrees to arrange such security clearances as may be required in order to provide such physical access. Service Provider shall ensure that its employees, agents, and subcontractors at all times comply with all applicable federal, state, county, local laws in the performance of the Services. Further, Service Provider will comply with this Agreement and applicable facility rules. Service Provider recognizes that its access to and usage of Company's resources such as, but not limited to, office equipment and supplies, computer network, software and hardware, data/voice/image storage and transmission are intended for authorized Company business use only and Service Provider and its personnel may be held personally responsible for any unauthorized use or disclosure. Service Provider shall use any such resources, including software, network and computer equipment only in connection with the performance of the Services. Service Provider recognizes that Company does not and cannot guarantee the privacy of files, information and messages stored in Company-owned files, desks, storage areas, or electronic media. For various reasons including maintenance, security, business, legal, compliance or regulatory requirements, authorized Company personnel must have unrestricted access to information stored in or on Company property or equipment. Any original documents, electronic records, files or records (including building access badges) which Company provides to Service Provider are and shall remain the sole property of Company. Service Provider shall return or destroy such property to Company within thirty (30) days after receiving Company's request and after the earlier of the termination of this Agreement or any individual Statement of Work.

2.3 **Company Subsidiary, Company Affiliate and Division Participation.** Company acts on behalf of itself and for its Affiliated member companies and divisions of such member companies, all of which are part of the AEGON Group (for purposes of this Section only, "Company Affiliate"). Company reserves the right to extend the benefits, obligations and privileges of this Agreement to each Company Affiliate even though each such Company Affiliate is not specifically named as a party to this Agreement. Each such Company Affiliate may execute a separate Statement of Work for Services, subject to the terms and conditions of this Agreement, and all such terms and conditions applying to Company shall apply to the Company Affiliate as if it was an original party to this Agreement, in which event: (i) the agreement between Service Provider and such Company Affiliate shall consist collectively of this Agreement and the Statements of Work(s) between Service Provider and such Company Affiliate, and (ii) such agreement shall constitute a separate, bilateral professional services agreement between Service Provider and such Company Affiliate. Further, each such Company Affiliate shall be individually responsible for its own payment and any obligation incurred under this Agreement. The failure of one Company Affiliate to satisfy its obligations under this Agreement shall in no way affect the performance or obligations between Service Provider and any other participating Company Affiliate, and the obligations of Company and such Company Affiliates to Service Provider shall in all events be several, and not joint and several.

3. **SERVICES**

3.1 **Services.** Service Provider shall provide Services under this Agreement in accordance with the applicable Statement of Work(s) agreed to by the parties and issued hereunder.

3.2 **Statement of Work.** All Services to be performed hereunder are to be specifically identified in Statements of Work as described herein. A separate Statement of Work will be prepared for each significant project mutually agreed to be undertaken in connection with this Agreement. Services performed in connection with any Statement of Work are deemed to be Services performed in connection with this Agreement. A template Statement of Work is attached as Exhibit A.

3.3 **Contents.** Except for minor tasks, which may be addressed in summary form, each Statement of Work may generally contain the following items:

- (a) A detailed description and/or Specifications of the Services to be performed and the Deliverables;
- (b) Completion and acceptance criteria to be applied in order to confirm that any Deliverables and/or Services meet the applicable Specifications;
- (c) A description of any work, Services or other items to be provided by Company or Service Provider;
- (d) The identity of, and contact information for, a project manager for each of Service Provider and Company (collectively "Project Managers");
- (e) The amount, schedule and method of payment;
- (f) An Implementation Schedule setting forth a timetable for delivery of Deliverables, acceptance testing, acceptance and other key milestones;
- (g) The term of the Statement of Work;
- (h) Such other terms and conditions as may be mutually agreeable between the parties; or
- (i) Any resources each party will provide.

3.4 **Adoption of Statement of Works and Changes.** Each Statement of Work will be effective only if in writing, approved, and signed by each party.

3.5 **Formalities.** Each Statement of Work shall reference this Agreement. The contents of the Statement of Work may be included in the body of the Statement of Work, or in separately signed attachments, as the parties consider most practical. It may also refer to or incorporate by reference other documentation that has been separately signed by the parties, such as all or a portion of any other Statement of Work that the parties have adopted. Each Statement of Work and changes to a Statement of Work are to be effective only if in writing accompanied by dated signatures of officers of each party. Service Provider is not authorized to provide to Company or to commit Company to procure any Services except in accordance with a signed Statement of Work.

3.6 **Project Managers.** The parties' Project Managers designated in a Statement of Work are responsible for:
(a) arranging all meetings, visits and consultations between the parties about such Statement of Work;
(b) receiving all notices and reports about such Statement of Work; and
(c) all administrative matters such as processing of invoices, payments, amendments and change orders to a Statement of Work.

3.7 **Modes of Payment.** Modes of payment for all Services and Deliverables shall be set forth in each Statement of Work or Exhibit D attached hereto. The rates stated in Exhibit D shall be effective for two (2) years from the Effective Date. Unless otherwise notified by Company at least thirty (30) days before the end of the then current term, this Agreement shall renew automatically for an additional one (1) year term at the then current term, plus any increase in fees agreed to in writing by the parties. If Service Provider is unwilling to renew this Agreement at the rates then in effect, it must notify Company at least sixty (60) days before the end of the then-current term of any proposed price increase. Any price increase after the first two (2) years shall be limited to the annual increase in the prior year's Consumer Price Index-Core (CPI) Index as published monthly by the Bureau of Labor Statistics, US Department of Labor or 3%, whichever is lesser.

3.8 **Implementation Schedules.** Service Provider shall use all commercially reasonable efforts to complete the Services and Deliverables according to the Implementation Schedule. Service Provider shall also prepare and submit such further reports of its performance and progress as Company may reasonably request from time to time.

3.9 **Incorporation of this Agreement by Reference; Precedence.** Each Statement of Work is deemed to incorporate the terms and conditions of this Agreement by reference. In the event of any express conflict or inconsistency between the provisions of a Statement of Work and the provisions of this Agreement, this Agreement controls unless the Statement of Work explicitly identifies the section of this Agreement that is superseded by the Statement of Work. Any change to a Statement of Work that follows the requirements of this Section will only apply to that Statement of Work.

3.10 **Change Orders.**
(a) **Right to Request Changes.** Either party may propose to reduce, alter, amend, enhance, or add to the scope or nature of the Deliverables to be provided under this Agreement or any Statement of Work or to modify the time or place of performance hereunder.

(b) **Procedure.** If either party proposes a change in a Statement of Work, such party shall provide a written change order ("Change Order") to the Project Manager of the other party. The request must be clearly identified as a proposal or request for a Change Order and provide information regarding the change comparable to the detail originally included in the applicable Statement of Work, including a description of the anticipated impact on the Services to be performed. If Company proposes a change, then within ten (10) business days after Service Provider's receipt of the proposal from Company, Service Provider shall advise Company of pricing or other terms that Service Provider believes will be affected by the proposed changes. Only a material change in a Statement of Work may result in a pricing change. If the proposed terms are not acceptable to Company, Service Provider and Company shall endeavor to agree upon appropriate and mutually agreeable changes in price, timing or other terms associated with the Change Order. If Service Provider and Company cannot agree upon such changes within twenty (20) business days after Service Provider's receipt of the notice of proposed changes from Company, the Services will continue with no change. While such changes are under review, Service Provider shall continue to perform the Services. Service Provider agrees to act in a commercially reasonable manner with regard to terms it requires for any proposed change. Service Provider shall evaluate proposed Change Orders at no additional charge to Company.

(c) **Right of Refusal.** Service Provider may not decline any Change Order that increases the cost or magnitude of performance, provided that the changes are reasonable in scope and a commensurate increase in compensation is fixed. Except as otherwise provided in this Agreement, neither party will be obligated to agree to any change in the Services and the provisions of this Section 3.10 set forth the only manner in which such changes to the Services may be accomplished. Each party agrees to act in good faith with respect to changes proposed by the other party.

3.11 **Reports.** Without limiting Service Provider obligations elsewhere in this Agreement, Service Provider will provide Company and its Affiliates with access to secure web based reports and statistical information with respect to Service Provider performance of the Services as Service Provider and/or Company or its Affiliates may reasonably deem necessary to apprise Company and its Affiliates adequately of Service Provider performance of the Services.

3.12 **Communications.**

(a) **Representations about Company and its Affiliates.** Service Provider hereby acknowledges that Company and its Affiliates are regulated by many governmental authorities ("Governmental Authorities"), and that performance hereunder may be subject to laws, regulations and policies enforced by Governmental Authorities. Neither Service Provider nor any of its Representatives shall make any oral or written representation relating in any way to Company and/or its Affiliates to any Governmental Authorities.

(b) **Representations about the Policies.** Service Provider shall not make any representations or other statements of any kind to Policyholders or any other person about the Policies, the coverage provided under the Policies or any of them, or any Policyholder's eligibility for benefits under a Policy.

3.13 **Nondiscrimination.** Service Provider will not discriminate because of age, sex, race, religion, color or national origin in its operations and provision of Services to any Policyholder.

3.14 **No Preferred Provider Arrangement.** Service Provider, in its performance of Services, is not and does not constitute a preferred provider arrangement, preferred provider organization, health maintenance organization, managed care plan or similar plan, network or arrangement.

3.15 **Books and Records.** Service Provider shall maintain or cause to be maintained those books, data, records and files required to reflect the Services (collectively, the "Records") in accordance with Supplier's policies or such longer period as required under applicable law. Company and its Affiliates shall have the right to inspect and audit Service Provider, Records during normal business hours by providing notice to Service Provider at least thirty (30) days prior to the date of the inspection or audit. Those Governmental Authorities exercising authority over Company and/or its Affiliates similarly shall have access to the Records as may be required by law or reasonably requested by Company and/or its Affiliates, and/or the Governmental Authorities.

- 3.16 **Lawsuits and Other Claims.** Service Provider shall notify Company and its Affiliates in writing within three (3) business days after Service Provider becomes aware of: (i) the institution or commencement of any claim, cause of action, suit, investigation or proceeding (including without limitation a disciplinary proceeding instituted or commenced by any Governmental Authority) in connection with Service Provider performance of the Services or any other obligation under this Agreement, or (ii) any communication threatening litigation against Service Provider and/or Company and/or its Affiliates in connection with Service Provider performance under this Agreement.
- 3.17 **Disposal and Destruction of Proprietary Information.** Service Provider agrees to comply at all times with Company's reasonable requests for disposal and destruction of any of Company's Proprietary Information, including, but not limited to, the following guidelines for:
- (a) Prior to destruction, all Proprietary Information will be secured against unauthorized access;
 - (b) Proprietary Information on Film: physical destruction through chemical, melting, incineration, or shredding with cross cut - no larger than 5/32" x 4/5";
 - (c) Proprietary Information on Magnetic Media or Solid State: bulk erase (except for hard drives) through destructive write or secure deletion/erasure;
 - (d) Proprietary Information on Magnetic Media or Solid State: physical destruction through hammer mill, shredding, or overwrite with high values (binary 1's), low values (binary 0's), or random bit patterns; and
 - (e) Proprietary Information on Optical Media: physical destruction through incineration, melting, or shredding.

4. **FEES AND PAYMENTS**

4.1 **Fees.** In consideration for providing Services hereunder, Company shall pay in U.S. dollars to Service Provider the Service Fees pursuant to the terms set forth herein and in each applicable Exhibit or Statement of Work. Except as otherwise agreed in writing by both parties, the payment described in a Statement of Work is to be the sole compensation to Service Provider for the performance of Services thereunder.

4.2 **Invoices and Payment.** Service Provider shall invoice Company for the prices, charges, taxes and reimbursable items payable to Service Provider as the conditions to payment are satisfied, with such supporting documentation as Company reasonably requests. If the invoice is valid and undisputed, Company shall pay the invoiced amount by the 30th day following receipt, unless a different time for payment is described in the Statement of Work. Invoices are to be addressed to the appropriate underwriting area for payment as defined by Company. Each invoice is to provide in reasonable detail the particular Services performed. Any extraneous terms on Service Provider's invoices are void and of no effect. In the event of any good faith dispute with regard to a portion of an invoice, the undisputed portion is to be paid according to the procedures described in this Section 4.2.

4.3 **Expenses.** In the event that a Statement of Work provides for the reimbursement of Service Provider's expenses in connection with performing Services thereunder, such reimbursement is limited to actual out-of-pocket expenses reasonably incurred that are pre-approved by Company in an Exhibit or Statement of Work, including travel expenses (e.g., airfare, local transportation, lodging and meals) and miscellaneous expenses (e.g., reproduction and shipping costs of materials). Service Provider shall provide a concrete plan for managing such costs. All expenses, including per diem expenses, are to be in accordance with Company's generally applicable policies (at actual cost to Service Provider) and must be approved in advance. Air travel is to be by coach or economy class only. Service Provider's policies for reimbursement of employee or contractor travel and living expenses are subject to Company's review and approval. Upon reasonable request, Service Provider shall provide Company with supporting documentation (such as receipts for travel, hotels and rental cars) with regard to such reimbursable expenses. Service Provider agrees to use the same diligence in controlling reimbursable expenses as it uses in its own business for expenses incurred by Service Provider, but in no event is Service Provider to use less than commercially reasonable diligence.

4.4 **No Other Payment.** Except as expressly provided in this Agreement or the applicable Statement of Work, Service Provider and Company shall each bear all of its own expenses arising from the performance of its

obligations under this Agreement, including, without limitation, personnel, facilities, utilities, equipment, supplies, clerical and the like.

4.5 **Annual Review of Fees.** The parties shall review all amounts due under this Agreement at least annually.

4.6 **Adjustment for Errors.** All payments made under this Agreement are subject to adjustment in the event of an error affecting such payment. Appropriate adjustments will be made within thirty (30) days after receipt of written notice of the error.

5. **PROPRIETARY RIGHTS/CONFIDENTIALITY/PRIVACY/SECURITY BREACH**

5.1 **Company Ownership of Deliverables.** Company shall have sole ownership of all right, title and interest in any Deliverables produced by Service Provider and its Representatives as a result of the Services performed under this Agreement. Service Provider agrees that any and all Deliverables produced by Consultant hereunder belong exclusively to Company and are Company Proprietary Information.

5.2 **Assignment of Intellectual Property Rights.**

(a) **Works for Hire.** All Deliverables are deemed works for hire. To the extent that any Deliverables may not, by operation of law, be works made for hire, Service Provider hereby irrevocably assigns to Company, and to the extent applicable shall require its Representatives to assign to Company, all patent, copyright and other proprietary rights of any kind in, to and under the Deliverables. Except as provided below in Sections 5.3 or 5.5, no rights are reserved for Service Provider.

5.3 **Ownership of Pre-existing Works.** Service Provider retains ownership of any pre-existing software or work of authorship which is incorporated into the Deliverables provided to Company hereunder, but with respect to such pre-existing software or works of authorship which are not otherwise licensed to Company under other agreements, Service Provider hereby grants to Company a royalty free, non-exclusive, perpetual, sub-licensable license to use, modify or create derivative works of such pre-existing software or works of authorship in connection with Company's use of the Deliverables. Any pre-existing software or works of authorship must be identified in the applicable Statement of Work for ownership to remain with Service Provider.

5.4 “INTENTIONALLY DELETED”

5.5 **Proprietary/Confidential Information.**

(a) **Protection of Proprietary Information.** If Proprietary Information is disclosed to a party (“Receiving Party”) by the other party (“Disclosing Party”), then Receiving Party agrees that it shall hold such Proprietary Information in confidence, agrees not to disclose any Proprietary Information to persons not having a need to know such Proprietary Information consistent with the purpose for which it was transmitted and such Proprietary Information will not be used, directly or indirectly, for any nonprofit, commercial, business or other purpose or in any way detrimental to Disclosing Party. Receiving Party shall take reasonable precautions to protect the confidentiality and value of Proprietary Information to Disclosing Party including measures to prevent loss, theft and misuse. Receiving Party shall give notice to Disclosing Party of any unauthorized use or disclosure of Proprietary Information, as soon as reasonably practicable. Receiving Party agrees to assist Disclosing Party in remedying any unauthorized use or disclosure of Proprietary Information caused by such Receiving Party.

(b) **Protection of Policyholder Confidential Information by Service Provider.** Except to the extent directly required to perform a legal duty, its obligations under this Agreement or as otherwise specifically authorized in writing by Company and its Affiliates or the Policyholder to whom such information relates, Service Provider shall hold in strictest confidence and not disclose to any Person at any time, whether during or after the term of this Agreement any Confidential Information in any form, whether, written, oral or electronic, directly or indirectly related to Policyholders. Service Provider shall apply at least the same standard of care to protect the confidentiality of Confidential Information as it uses to protect its own confidential information. Service Provider shall not use Confidential Information for any purpose except to the extent specifically provided for in this Agreement.

- (c) Provision of Policyholder Confidential Information to Service Provider. Company and its Affiliates may provide Service Provider with Policyholder Confidential Information reasonably necessary to the provision of the Services.
- (d) Business/Regulatory Record Exception. Each party acknowledges the information contained in notes, correspondence and reports prepared by a party in connection with the party's discussions are business records of the Receiving Party. Each party agrees that business records and Proprietary Information retained for any regulatory requirement or as part of an automatic journaling or retention system need not be returned or destroyed, but are subject to all other terms of this Agreement.
- (e) Return of Proprietary Information. Upon written request of a party, each party shall promptly as possible (and in any event within thirty (30) days) return or destroy (as directed by the Disclosing Party) all Proprietary Information received from the other party, including all copies, except to the extent such return or destruction is not feasible, and except Proprietary Information Receiving Party is entitled to retain under Section 5.5(d). Upon the request of the Disclosing Party, the Receiving Party shall furnish to the Disclosing Party an affidavit providing assurances as to the return or destruction of the Disclosing Party's Proprietary Information.
- (f) Disclosure Required by Law. In the event that Service Provider receives a request to disclose all or any Proprietary Information under the terms of a subpoena or order issued by a valid court or other governmental body (including without limitation any department of insurance), or any other request for disclosure of Proprietary Information, Service Provider agrees, if permitted by Applicable Law: (i) to notify Company as soon as reasonably practicable after Service Provider receives the request, and in any event prior to responding thereto, of the existence, terms and circumstances surrounding such request; (ii) to consult with Company on the advisability of taking legally-available steps to resist or narrow such request; and (iii) if disclosure of Proprietary Information is required to prevent Service Provider from being held in contempt or subject to other penalty, to furnish only such Proprietary Information as Service Provider is advised by outside counsel that it is legally compelled to disclose and to exercise its best reasonable efforts to obtain assurance that confidential treatment will be accorded to the disclosed Proprietary Information.
- (g) HIPAA Covered Products. Service Provider and its Representatives shall comply with (a) all Applicable Law respecting the confidentiality of Policyholder information and data concerning Policyholders acquired in the course of Service Provider performance of its obligations under this Agreement, including, but not limited to, HIPAA and regulations promulgated thereunder, and (b) with other confidentiality provisions set forth in this Agreement.

5.6 **Prohibition of Use of Company Name and Trademarks.** Each party shall not use the name, trademark, trade dress, logo or other indicia of origin of the other party or any Affiliate of the other party (collectively, "Name") in advertising or sales materials or in any other manner whatsoever without prior express written approval of the party owning such Name, except in furtherance of performing Services or satisfying legal duties. Such prohibition includes, without limitation, the following:

- (a) Each party shall not refer to the existence of this Agreement without the other party's prior express written approval;
- (b) Each party's use of the other party's Name is strictly limited to meeting disclosure obligations imposed by regulatory bodies, such as the SEC or FINRA;
- (c) Each party is not allowed to make any statement or representation whatsoever regarding the other party's company, product or services without the first party's prior express written approval; and
- (d) If a party provides prior express written approval for the use of its Name, such party further reserves the right to revoke such approval at any time.

5.7 **Ownership.** Except as provided in this Agreement or any Statement of Work, all materials transmitted between the parties are to remain the sole and exclusive property of the Disclosing Party to the extent that they contain Proprietary Information. Except for the licenses or ownership rights granted in this Agreement, this Agreement and transmission or disclosure of any Proprietary Information does not grant the Receiving Party a license or ownership of any type.

5.8 **Expiration of Obligations.** All obligations and restrictions of confidentiality under this Agreement are to remain in effect for a period of seven (7) years following the date of disclosure for Confidential Information, and with respect to Trade Secrets pursuant to applicable law, for as long as such information remains a Trade Secret. All obligations of confidentiality and all restrictions on the use of Personal Information and Protected Health

Information under this Agreement are to remain in effect for as long as such information remains Personal Information (as that term is defined in Section 5.11) or Protected Health Information. Such time periods may be extended upon written agreement of the parties.

5.9 **Responsibility for Affiliates and Representatives.** Each party is solely responsible for any breach of this Agreement by its Representatives including, without limitation, any improper use or disclosure by its Representatives of the other party's Proprietary Information. Receiving Party may disclose Proprietary Information to its Representatives who in Receiving Party's reasonable judgment have the need to know such information in connection with this Agreement. Receiving Party shall inform its Representatives of the confidential nature of such Proprietary Information, shall direct them to hold Proprietary Information in strict confidence, shall take all reasonable precautions to prevent improper use of Proprietary Information by them, and shall be responsible for any breaches by them of the terms found in this Agreement.

5.10 **Proprietary Legends.** Neither party shall remove or obscure the proprietary legends or marks appearing on materials provided by the other party.

5.11 **Privacy.**

For purposes of Sections 5.11, 5.12 and 5.13 only, the following definitions shall apply:

"Applicable Privacy Law" means any law, ordinance, statute, rule or regulation applicable to or binding on either party with respect to privacy or data security, including but not limited to the Health Insurance Portability and Accountability Act of 1996 "HIPAA" and all related regulations issued pursuant to the Act, the Health Information Technology for Electronic and Clinical Health Act ("HITECH") and all related regulations issued pursuant to the Act, the Gramm-Leach-Bliley Act (Pub. L. 106-102) ("GLBA"), Regulation S-P (17 CFR 248), the Fair and Accurate Credit Transactions Act of 2003 (Pub. L. 108-159), and the Standards for the Protection of Personal Information of Residents of the Commonwealth of Massachusetts (210 CMR 17), as each may be amended from time to time.

"Personal Information" means, in addition to any definition under Applicable Privacy Law, any personally identifiable information about any individual, including, but not limited to, name, email address, telephone number, age or date of birth, gender, zip code, demographic information, marketing preferences, social security number, alien identification number, credit or debit card numbers, other financial account numbers, application data, credit history, financial information, drivers license number, other unique identifier or authenticator, health insurance or medical information, consumer report information and data about transactions or experiences with Company or marketing partner of Company. The term "individual" for purposes of this definition includes, but is not limited to a customer, client, employee or contractor of Company. Personal Information includes Nonpublic Personal Financial Information, Electronic Protected Health Information, and Protected Health Information.

"Security Breach" means any actual or potential breach under Applicable Privacy Law with respect to any record or data containing Personal Information or Protected Health Information, and shall include any incident involving the unauthorized access to or acquisition of Personal Information, whether it be encrypted or unencrypted, or in electronic or paper copy, or where the potential exists that encrypted Personal Information or Protected Health Information could be compromised. In the event of any actual or suspected breach involving Protected Health Information, the term Security Breach shall include "breach" as defined in Section 13400 of the HITECH Act (as amended or superseded from time to time), a violation of any provisions under Section 5.12 of this Agreement, the occurrence of a "security incident" as defined in 45 C.F.R. Section 164.304, or any potential or actual security breach or incident as defined by applicable state law.

(a) **Disclosure and Use of Personal Information.** If Service Provider receives, uses, stores, maintains, processes, transmits, disposes or otherwise has access to Personal Information, Service Provider shall use, store, maintain, process, transmit, dispose of and protect Personal Information in accordance with Applicable Privacy Law. Access to and use of Personal Information by Service Provider is specifically limited to that which is necessary to perform the Services set forth in this Agreement and disclosure of Personal Information should be made only to those individuals who have a need to know such information to perform the Services. Service Provider shall obligate its representatives to comply with terms that are at

least as stringent as, and consistent with, those set forth in this paragraph. If Service Provider is required by law to disclose Personal Information, Service Provider shall promptly notify Company in writing (unless prohibited by law) in advance of such disclosure, and provide Company with copies of any unprivileged information to be disclosed to permit Company to take action, if necessary, to object to the release of the Personal Information and Service Provider shall reasonably cooperate with Company in seeking a protective order or other agreement to maintain the confidential nature of the information. At any time that Company requests, if feasible, Service Provider shall securely dispose of all records, electronic or otherwise (including backup records or copies), regarding or including any Personal Information that Service Provider may then possess or control. Disposal may be achieved, at Company's option, through delivery of the records to Company or destruction in a manner that renders the records unreadable and undecipherable by any means. Service Provider agrees to certify in writing to Company that all such Personal Information has been securely destroyed or returned. Further, Service Provider shall comply with Company's Information Security Requirements attached hereto as Exhibit B.

(b) Information Security Program. Service Provider shall develop and implement, within thirty (30) days after the date of execution of this Agreement, if it has not already done so, and thereafter maintain, a comprehensive written information security program that contains administrative, technical, and physical safeguards compliant with Applicable Privacy Law (the "Security Program") designed to: (i) protect the confidentiality, integrity and availability of Personal Information; (ii) protect against anticipated threats or hazards to the security, confidentiality, integrity and/or availability of Personal Information; (iii) protect against any unauthorized access, disclosure or use of Personal Information; (iv) address computer and network security; (v) address physical security; (vi) address business continuity and disaster recovery; (vii) address a security incident response program; and (viii) provide for the secure destruction and disposal of Personal Information. The Security Program shall comply with all Applicable Privacy Law and shall be updated as required by Applicable Privacy Law and industry best practices. Service Provider shall require its contractors who provide services on behalf of Service Provider and who may have access to Personal Information ("Contractors") to develop, implement, and maintain a written Security Program and to provide Service Provider with written acknowledgement of compliance of Contractors' Security Program. Nothing herein should be construed to waive any requirement in any agreement between Service Provider and its Contractors for compliance with Company's security standards and requirements for Personal Information, privacy, data security and network/systems security communicated to Service Provider herein.

(c) Security Breach Reporting. Service Provider shall notify Company within forty-eight (48) hours upon learning of an actual or potential Security Breach involving Personal Information. Service Provider must provide notice to Company's Privacy Office by emailing the Project Manager and must include, at a minimum, and to the extent known, the following information: (a) the nature of the Security Breach; (b) the estimated impact on Company; (c) the name of a senior level person responsible for communicating with Company regarding the Security Breach; and (d) the investigative action taken or planned. Service Provider must reasonably cooperate with the Company's requests for information regarding the Security Breach and Service Provider must provide regular updates on each Security Breach and the investigative and corrective action taken. Any action taken with respect to such Security Breach, including, but not limited to, the investigation and any communication to internal or external parties regarding the Security Breach, will be at the sole discretion of Company unless otherwise required by Applicable Privacy Law.

(d) Indemnity. Service Provider hereby agrees to defend, indemnify, and hold Company and its Affiliates and all of their respective directors, officers, personnel, and their successors and assigns harmless from any and all expenses, damages, awards, settlements, claims, actions and causes of action (in each case regardless of whether sounding in contract, tort, or otherwise), demands, losses, obligations, fines, penalties, liabilities and regulatory actions (including, but not limited to, reasonable attorneys' fees and expenses, breach notification costs, credit monitoring or watch services, internal and external breach remediation plans) arising out of or relating to any privacy or security breach of Personal Information in the possession of or under the control of the Service Provider or its Representatives which is caused by them, or for Service Provider's breach of any obligations set forth in this Section.

5.12 HIPAA and HITECH Privacy and Security Obligations For HIPAA Covered Products

If the Services relate to any HIPAA-covered products, Service Provider shall comply in full with the privacy and security requirements issued pursuant to HIPPA and HITECH as any of the same may be amended or superseded from time to time, including, without limitation, the requirements forth below:

- (a) For the purposes of this Section only, "Individual" means a consumer who is the subject of PHI and seeks to obtain, obtains, or has obtained financial or insurance products or services which are to be used primarily for personal, family, or household purposes.
- (b) Service Provider agrees and acknowledges that it is directly subject to HIPAA (as amended by the HITECH Act and as may be amended or superseded from time to time), including Sections 164.308, 164.310, 164.312 and 164.316 thereof, including its provisions relating to security and privacy of PHI as well as its enforcement and penalty provisions. Service Provider agrees that it shall (i) comply with all applicable security and privacy provisions of HIPAA, as well as all applicable state and local laws and regulations enacted to protect the privacy and security of Individuals' PHI (as any of the same as may be amended or superseded from time to time); and (ii) not act in any way to interfere with or hinder the Company's ability to comply with HIPAA.
- (c) Except to the extent otherwise required or specifically permitted by law, or to the extent specifically provided herein, Service Provider's use and/or disclosure of PHI shall be limited solely to the purposes of performing Services under this Agreement, for the proper management of Service Provider's business to carry out Service Provider's legal responsibilities, or otherwise as required by law.
- (d) In response to an unsolicited direct Individual's inquiry, Service Provider may disclose PHI directly to, and may discuss such information directly with, the Individual to whom such information pertains, provided that such disclosure would not violate HIPAA if Company made it.
- (e) Service Provider may not disclose any PHI to a Nonaffiliated Third Party (as defined under 15 U.S.C. §6809(5) and as amended or superseded from time to time), including but not limited to Service Provider's sub-agents, vendors, contractors, and/or subcontractors, unless such disclosure would be lawful if made directly to the Nonaffiliated Third Party by us. Service Provider agrees and understands that any such disclosure is subject to HITECH, including those provisions related to the sale and marketing of PHI.
- (f) Service Provider shall require that Service Provider's sub-agents, directors, officers, vendors, contractors, Subcontractors and/or employees to whom Service Provider provides, or who otherwise receives PHI to agree in writing to the same restrictions and conditions that apply to Service Provider with respect to such information; provided, however, that Service Provider shall be entitled to provide PHI only to such of its sub-agents, directors, officers and employees who need such PHI to enable them to perform under this Agreement, and then only to the extent necessary for such purpose.
- (g) Service Provider represents and warrants that it and any Subcontractors used in providing the Services shall comply with applicable state and federal privacy and security laws. Service Provider shall enter into written business associate contracts (including the terms required under HIPAA) with each Subcontractor prior to any such Subcontractor having access to Policyholders or any information about Policyholders.
- (h) Service Provider may not use or disclose Protected Health Information in any manner that would constitute a violation of 45 C.F.R. Parts 160 and 164 or 13405(d) of the HITECH Act.
- (i) At the request of and in the time and manner designated by Company, Service Provider shall cooperate with Company in responding to any Individual's (i) request for access to their PHI, and/or (ii) request to amend their PHI.
- (j) Service Provider shall keep a written record of disclosures of PHI that must be provided in an accounting under HIPAA to an individual to whom the PHI relates ("Disclosures"), and shall comply with any request by Company to provide Company with such information regarding such Disclosures, and in such format, as Company reasonably may request.
- (k) In the event that Service Provider receives a request to disclose all or any PHI under the terms of a subpoena or order issued by a court or other governmental body (including without limitation any department of insurance), or any other request for disclosure of PHI, Service Provider agrees: (i) to notify Company of the existence, terms and circumstances surrounding such request within three (3) business days after Service Provider receives the request, and in any event prior to responding thereto, (ii) to comply with any reasonable requests by Company to assist Company in responding to such legal document.
- (l) Service Provider shall limit Service Provider's disclosure of PHI to the minimum necessary for the particular purpose of each disclosure. Service Provider shall only collect such information as is necessary to perform its Services under the Agreement.
- (m) Service Provider represents and warrants that it has implemented and shall maintain administrative, physical and technical safeguards (the "Safeguards") designed to prevent prohibited uses or disclosures, and to protect the confidentiality, integrity and availability, of PHI that Service Provider creates, receives, maintains or transmits. Such safeguards shall include development, implementation, and maintenance of a comprehensive written information security program compliant with Applicable Privacy Law and designed

to (i) protect the integrity and confidentiality of PHI, (ii) protect against anticipated threats or hazards to the security, confidentiality and/or integrity of PHI, (iii) protect against any unauthorized, disclosure, or use of PHI, (iv) address computer and network security, (v) address physical security, and (vi) provide for the secure destruction and disposal of PHI.

(n) In the event Service Provider determines that disclosure of PHI to Service Provider's sub-agents, vendors, contractors, and/or subcontractors is necessary in order to perform under the Agreement or comply with any obligation under this Agreement, Service Provider shall ensure that such sub-agents, vendors, contractors, and/or subcontractors have implemented reasonable and appropriate administrative, physical and technical safeguards to protect PHI.

(o) Service Provider agrees to use its best reasonable efforts to notify Company in writing without delay and in any event within 48 hours upon discovering any Security Breach including (i) a "breach," as the term "breach" is defined in Section 13400, and as the terms "breach" and "discover" are further described in Section 13402(c), of the HITECH Act, (ii) a violation of any provisions under Section 1 of this Agreement, (iii) the occurrence of a "security incident," as defined in 45 C.F.R. Section 164.304, or (iv) a potential or actual security incident as defined by applicable state law. Further, any report of a security incident from Service Provider to Company shall describe the remedial or other action undertaken by Service Provider to correct the current security incident and to prevent future security incidents.

(p) If a security incident or Security Breach occurs, Service Provider shall take reasonable steps to mitigate the adverse impact of the security incident and to prevent future security incidents. Similarly, Service Provider shall mitigate, to the extent practicable, any harmful effect that is known to Service Provider that results from any access, use, disclosure, modification or destruction of PHI in violation of this Agreement.

(q) In the event of an actual or suspected breach or security incident, Service Provider agrees to cooperate fully with Company in any incident investigation or resolution, and agree that no notifications and/or communications to any individual(s), media outlets, state or federal authorities, or other third parties regarding the breach will be made without Company's prior written consent (which consent shall not be unreasonably withheld, conditioned, delayed or denied), unless Applicable Law requires otherwise from Service Provider.

(r) In the event either party learns of a pattern of activity or practice of the other party that constitutes a material breach or violation of its obligations relating to PHI under this Agreement, the non-breaching party will take reasonable steps to cure the breach or end the violation.

(s) If Service Provider has breached Section 5.12 of this Agreement, Company may (i) provide an opportunity for Service Provider to cure the breach within the time specified by Company, or (ii) terminate this Agreement if Company has determined, in its sole discretion, that cure is not possible. If termination is not feasible, Company may report the problem to the Secretary of the U.S. Department of Health and Human Services (the "Secretary"). Notwithstanding the above, Company also reserves the right to terminate this Agreement, at Company's sole discretion, in the event of a material breach or security incident.

(t) Upon termination of this Agreement, if feasible, Service Provider shall return or destroy, in an appropriately secure manner, all PHI without retaining any copies and shall provide Company with Service Provider's written and signed certification to that effect. If such return or destruction is not feasible, Service Provider shall limit all further uses and disclosures to those purposes that make such return or destruction of the PHI not feasible.

(u) Service Provider shall make its internal practices, books and records relating to uses and disclosures of PHI available to Company (or to Company's designee) and to the Secretary, or to the Secretary's designee, for the purpose of confirming Service Provider's compliance and/or Company's compliance with 45 C.F.R. Parts 160 and 164 in connection with the transactions contemplated by this Agreement or as permitted by law.

(v) The parties can mutually agree to amend 5.12 of this Agreement to reflect (i) future amendments of HIPAA, (ii) court orders interpreting the application of HIPAA, or (iii) a material change in Company's business practices.

(w) At the request of and in the time and manner designated by Company or its Affiliates, Service Provider shall provide access to PHI then in its control or possession or in the possession or control of its Subcontractors or vendors to Company or its Affiliates, or, as directed by Company or its Affiliates, to a Policyholder. If a Policyholder contacts Service Provider directly about access to his or her PHI, Service Provider shall not provide such access, but rather shall forward such request to Company and its Affiliates

in writing within five (5) days after having received the request. Notwithstanding the above, Service Provider shall cooperate with Company and its Affiliates in responding to any such request.

(x) At the request of and in the time and manner designated by Company and its Affiliates, Service Provider shall amend PHI in its possession or control or in the possession or control of its vendors and/or Subcontractors. If a Policyholder contacts Service Provider directly about amending his or her PHI, Service Provider shall not make such amendment but rather shall forward such request to Company and its Affiliates within five (5) business days after having received the request. Notwithstanding the above, Service Provider shall cooperate with Company and its Affiliates in responding to any such request.

(y) Service Provider shall comply with such other restrictions on the use or disclosure of Protected Health Information as required under 45 C.F.R. §164.504(e), as may be amended from time to time or as may be required under any controlling judicial, quasi-judicial or administrative decision, ruling, opinion, policy or other authority with respect to 45 C.F.R. §164.504(e).

(z) The provisions of Section 5.12 of this Agreement shall survive the termination of this Agreement and/or the return or destruction of PHI.

(aa) Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits compliance with HIPAA.

(bb) Service Provider obligations with respect to Protected Health Information shall survive the termination of this Agreement and/or the return or destruction of any Protected Health Information and shall survive until the fifth (5th) anniversary of termination of this Agreement or the sixth (6th) anniversary of the last date on which Services are provided by Service Provider, whichever is later.

5.13 **Compliance with GLBA.** Service Provider shall comply with the privacy requirements of the GLBA and the rules and regulations promulgated thereunder (as any of the same may be amended or superseded from time to time, "GLBA"), as set forth below:

(a) Except to the extent otherwise required or specifically permitted by law, or to the extent specifically provided herein, Service Provider use and/or disclosure of Policyholder Confidential Information shall be limited solely to the purposes for which it is disclosed to Service Provider to perform its obligations under this Agreement.

(b) Service Provider shall require that its agents, directors, officers, and employees to whom it provides, or who otherwise receive Policyholder Confidential Information to agree to substantially the same restrictions and conditions that apply to Service Provider with respect to such information.

(c) Service Provider shall implement appropriate measures to ensure the security and confidentiality of Policyholder Confidential Information.

6. **WARRANTIES**

6.1 **Deliverables.** Service Provider represents and warrants that all Deliverables, when accepted, will meet the applicable Specifications set forth in the applicable Statement of Work. Any tools used in conjunction with the Deliverables will be tested for value, security, and appropriateness to the task prior to being used. Unless otherwise set forth in a SOW, within ninety (90) days from the date of Company's receipt of the Deliverables, Service Provider warrants that it will correct, without charge to Company, any Deliverables that fail to conform in accordance with the applicable Statement of Work.

6.2 **Services.** Service Provider represents and warrants that all Services will be performed in a competent, professional and workmanlike manner and in conformity with the requirements set forth in each applicable Statement of Work or in any exhibits or schedules attached thereto and consistent, competent, professional manner and in accordance with the terms of this Agreement, Applicable Law, and industry standards. Unless otherwise set forth in a SOW, within ninety (90) days from the date of Company's receipt of the Services, Service Provider warrants that it will correct, without charge to Company, any Services that fail to conform to the applicable Statement of Work.

6.3 **Sufficient Resources.** Service Provider represents and warrants that it shall provide sufficient employees and facilities to perform its obligations under this Agreement to perform the Services within the applicable time frames agreed to by the parties and that such employees have sufficient skill, knowledge and training to perform the Services.

6.4 **Intellectual Property Assignments.** Service Provider represents and warrants that: (i) all Employees and Representatives utilized by Service Provider in performing Services for Company are under a written obligation to Service Provider requiring such persons to maintain the Proprietary Information of Service Provider's customers and (ii) with respect to Employees, to assign all of such person's right, title and interest to Service Provider in and to any Services and Deliverables which are developed, prepared, conceived, made or suggested by such person while providing Services on behalf of Service Provider. In addition, prior to commencement of any work under this Agreement, Service Provider shall require all Employees and Representatives utilized by Service Provider to individually sign a confidentiality and nondisclosure agreement with provisions as least as restrictive as those set forth in this Agreement.

6.5 **Actions, Suits or Proceedings.** Service Provider represents and warrants that there are no actions, suits, proceedings or investigations, pending or, to the best of its knowledge, threatened, that could have a material adverse effect on Service Provider's ability to fulfill its obligations under this Agreement. Service Provider further warrants that it shall immediately notify Company if, during the term of this Agreement, Service Provider becomes aware of any action, suit or proceeding, pending or threatened, that could have a material adverse effect on Service Provider's ability to fulfill its obligations under this Agreement.

6.6 **Non-Infringement.** Each party represents and warrants to the other party that any goods, services or information provided to the other party for its use pursuant to this Agreement, and Service Provider represents and warrants that the creation of any work product, including, without limitation, any of the Services or Deliverables, do not and shall not infringe any third party patent, copyright, Trade Secret, trademark or other Intellectual Property rights of any kind without limitation, and there is no actual or threatened claim or lawsuit by any third party for infringement of such rights. Each party further represents and warrants that it shall promptly inform the other party if, after the Effective Date of this Agreement, such party receives an actual or threatened claim or lawsuit by any third party based on a violation of such rights.

6.7 **Compliance with Applicable Law.** Service Provider represents and warrants that the Services and Deliverables being provided by Service Provider, as well as its employees, agents, representatives, affiliates and Subcontractors shall at all times comply with all Applicable Law. Service Provider further represents and warrants that it will have obtained any necessary permits, licenses, certificates or any other documentation and authorization required to comply with any such laws and regulations or for Service Provider to perform the Services and/or its other obligations under this Agreement. Company and its Affiliates represent and warrant that they will comply with all applicable laws, rules and regulations, and not use or disclose any of the Deliverables for any purpose not authorized in this Agreement.

6.8 **Virus Protection.** If any software is provided to Company as part of the Services or Deliverables, Service Provider represents and warrants that it shall use the most effective methods and techniques reasonably available to Service Provider to check the software, prior to delivery to Company, for the presence of Viruses and to remove and destroy any such Viruses found in the software and, to the best of Service Provider's knowledge at the time of submission, the software delivered hereunder contains no Viruses. If the installation of the software by Company transfers to Company's computers a Virus, Service Provider shall reimburse Company the reasonable cost incurred by Company including costs of persons employed by Company to remove and recover from such Virus.

6.9 **Absence of Disabling Devices.** If any software is provided to Company as part of the Services or Deliverables, Service Provider represents and warrants that none of the software contains, or will contain, any Self-Help Code or any undisclosed Unauthorized Code or similar malicious computer instructions, intentional devices or techniques that can or were designed to threaten, infect, attach, assault, vandalize, defraud, disrupt, damage, disable, improperly access, interfere with, cause damage to, or shut down a computer system or any component of such computer system, including its security or user data.

6.10 **Functionality of Programming.** Any software developed or delivered as part of the Deliverables shall conform to and perform in the computer environment agreed to by Service Provider and Company. This warranty may be immediately terminated if any modification is made to the source code by non-Service Provider personnel without Service Provider's consent or direction. Service Provider will charge Company for costs incurred and time spent, as set forth in Section 4, if the cause of error was not within the software as delivered or required to be delivered to Company. Service Provider further warrants that all Deliverables shall correctly function without additional modification, additional

programming, or manual intervention with regard to any use, handling, storage, processing, calculation, reference, or transference of information and/or data for any period of time after 1999. Service Provider warrants that the functionality of all Deliverables shall not be impaired, altered, or changed with respect to the use of data or records containing dates falling prior to, on or after January 1, 2000.

7. REMEDIES AND LIMITATIONS

7.1 **Material Breach.** In the event that either party commits a material breach of any provision of this Agreement, including, without limitation, any of the warranties set forth in Section 6 above, the other party is, unless otherwise provided for herein, entitled to avail itself of any and all legal and equitable remedies, including the right to terminate as set forth in Section 9.

7.2 **Nonconformity of Services.** In the event Company notifies Service Provider of any nonconformity with respect to the warranties set forth in Section 6, Service Provider shall, at its own expense, promptly re-perform the Service or correct such nonconformity as necessary to bring the Deliverable into conformity with the applicable Specifications. Service Provider's curative efforts are to be completed within fifteen (15) business days (the "Cure Period"), unless a different period is set forth in an applicable Statement of Work. In the event Service Provider is unable to cure such nonconformity within the Cure Period, Company may immediately terminate the applicable Statement of Work.

7.3 **Dispute Resolution.**

(a) **Negotiation.** Except where injunctive relief is sought, each party shall attempt in good faith to resolve any controversy, claim or dispute of whatever nature arising out of or relating to this Agreement or the breach, termination, enforceability or validity thereof ("Dispute") promptly by negotiation between executives or managers who have authority to settle the Dispute and who are at a higher level of management within each of the parties' organizations than the parties' appointed Project Managers. Each party shall provide the other with all unprivileged information and documentation relied upon by the party to substantiate its position with respect to the Dispute other than attorney work product.

(b) **Waiver of Right to Jury Trial.** If the parties are unable to resolve a Dispute using the mechanisms described above, then either party is entitled to any and all legal and equitable remedies available. However, Company and Service Provider agree not to seek, and each hereby waives any right to, trial by jury in any action, proceeding or counterclaim brought by either of them against the other on any matter or claim arising out of or in any way relating to this Agreement, a Statement of Work, the relationship of Company and Service Provider, the performance or non-performance of the Services, any claim of injury or damage, or the enforcement of any remedy under any law, irrespective of whether any such matter or claim is based in contract, in tort or otherwise. Neither party shall seek to consolidate any such action in which the right to trial by jury has been waived with any other action in which such right has not been or cannot be waived, it being the intention of the parties that the jury trial waiver be subject to no exceptions.

7.4 **Other Remedies.** Each party agrees and acknowledges that breach of this Agreement may cause the other irreparable harm without an adequate remedy at law and hereby agrees that the other party may seek temporary or permanent injunctive relief to prevent or limit the effect of any such breach.

7.5 **Attorney Fees.** If any dispute arises between the parties hereto concerning the breach, enforcement or interpretation of any provision of this Agreement, then the prevailing party shall be reimbursed its court costs, reasonable attorneys' and expert witness fees and disbursements, and all other costs and expenses incurred by the other party on account thereof, including those incurred in connection with any matters on appeal.

7.6 **Limitation of Liability.**

EXCEPT AS OTHERWISE STATED HEREIN OR FOR FRAUD, MALICIOUS, WILLFUL OR INTENTIONAL TORTIOUS ACTS; BREACHES OF CONFIDENTIALITY; OBLIGATIONS TO INDEMNIFY AND CLAIMS ARISING OUT OF OR RELATING TO PROPERTY DAMAGE, PERSONAL INJURY AND/OR DEATH, NEITHER PARTY'S TOTAL LIABILITY TO THE OTHER ARISING OUT OF OR RELATING TO THIS AGREEMENT, WHETHER BASED ON CONTRACT, TORT OR ANY OTHER LEGAL THEORY, SHALL NOT EXCEED FOUR TIMES THE AMOUNT OF FEES PAID AND TO BE PAID BY COMPANY AND ITS

AFFILIATES TO SERVICE PROVIDER DURING THE TERM OF THIS AGREEMENT. EXCEPT WITH RESPECT TO OBLIGATIONS TO INDEMNIFY, NEITHER PARTY BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, EXEMPLARY, PUNITIVE, SPECIAL OR SIMILAR DAMAGES INCLUDING, WITHOUT LIMITATION, LOSS OF PROFITS OR LOSS OF REVENUES, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE LIKELIHOOD OF THE OCCURRENCE OF SUCH DAMAGES OR SUCH DAMAGES ARE FORESEEABLE.

8. INDEMNITY

8.1 Indemnification for Service Provider Acts and Omissions. Service Provider, its Affiliates and successors in interest, shall and hereby does indemnify, defend and hold harmless Company and its Affiliates, and their respective shareholders, Representatives, successors and assigns harmless from and against any and all expenses, costs damages, claims, actions and causes of action (in each case whether sounding in contract, tort or otherwise), demands, losses, obligations, fines, penalties and liabilities (including, but not limited to, reasonable attorneys' fees and expenses) resulting in any manner from the performance or non-performance of Service Provider or its Affiliates, or any of their respective shareholders and Representatives (collectively, the "Service Provider Parties") arising out of (i) any breach by Service Provider Parties or those acting for or on behalf of Service Provider of any of Service Provider's obligations hereunder; (ii) any negligent or wrongful act or omission on the part of any of the Service Provider Parties in the performance or nonperformance of any duty or obligation required to be performed by Service Provider under this Agreement; (iii) fraud, bad faith, illegal act or omission, negligence (including professional negligence) or willful misconduct by Service Provider or its Representatives or any other person acting at the direction or under the control of Service Provider; (iv) any breach by any of the Service Provider Parties of the representations, warranties, duties and/or obligations of Service Provider under this Agreement; and (v) any act by Service Provider that is beyond the scope of its authority hereunder; provided that, any acts or omissions by Service Provider or its Representatives causing damage will not require indemnification to the extent arising from the willful or negligent acts of Company, its employees or agents.

8.2 Indemnification for Company Acts and Omissions. Company agrees to defend, indemnify and hold Service Provider and its shareholders, Representatives, successors and assigns harmless from any and all expenses, damages, claims, actions, demands, losses, liabilities and causes of action (including, but not limited to, attorneys' fees and expenses) to the extent arising out of or relating to a breach of this Agreement or Applicable Law, or the willful or negligent acts or omissions on the part of Company, its employees or agents, including, but not limited to, injury or death to all persons as well as damage to any real or personal property.

8.3 Personnel. Service Provider agrees to defend, indemnify and hold Company and its Affiliates and all of their shareholders, Representatives, successors and assigns harmless from and against any and all expenses, damages, claims, actions, demands, losses, fines, penalties, liabilities and causes of action (including, but not limited to, reasonable attorneys' fees and expenses) arising out of or relating to withholding taxes, unemployment or workers compensation, employee benefits or compensation, employment claims, or any other claim, demand, liability or loss of any nature relating to the personnel supplied to Company or providing Services to Company under this Agreement.

8.4 Indemnification for Intellectual Property Infringement.

(a) **Obligation to Indemnify.** Service Provider agrees to defend, indemnify and hold Company and its Affiliates and all of their shareholders, Representatives, successors and assigns harmless from and against any and all expenses, damages, claims, actions and causes of action (whether sounding in contract, tort or otherwise), demands, losses and liabilities (including, but not limited to, reasonable attorneys' fees and expenses) arising out of or relating to infringement or alleged infringement of any patent, copyright, Trade Secret, trademark or other Intellectual Property rights for or on account of the manufacture, distribution, sale or use of any results, Services or Deliverables furnished hereunder. Service Provider is not required to indemnify where (i) such matter arises due to Company's actions or omissions contrary to the documentation applicable to the Deliverables from which the infringement is claimed, or (ii) compliance by Service Provider with detailed specifications prescribed by or originating with Company that constitutes the basis of the infringement or alleged infringement.

(b) **Application to Software.** This Section 8.4 applies to any software licensed or used by Company as part of the Services described in any Statement of Work, including, without limitation, a pilot project or proof

of concept, until such time as any such software becomes the subject of a separate licensing agreement between Service Provider and Company that by its terms expressly supersedes the indemnification obligations in this Section.

8.5 **Conditions Precedent.** For any indemnification claim under Section 8, the party seeking indemnity shall promptly notify the other party in writing of any claim, demand, suit or proceeding, together with any and all documentation related to such claim, demand, suit or proceeding. The indemnifying party shall have full authority to control the defense of such suit at its expense; however no admission of liability on behalf of the indemnified party will be made without prior written consent from the indemnified party. The indemnifying party may not settle any claim unless the claimant gives a full unconditional release of all liability. The party seeking indemnification may participate at its own expense. The failure of a party seeking indemnity under this Section to provide the other party with prompt notice does not relieve the party providing indemnification of its obligations under this Section 8, unless such failure to promptly notify the party providing indemnity causes such party material prejudice. No settlement that prevents Company from continuing to use the results, Services and Deliverables shall be made without Company's prior written consent, which consent shall not be unreasonably withheld, conditioned, delayed or denied.

9. **TERM AND TERMINATION**

9.1 **Term of Agreement.** This Agreement is to commence as of the Effective Date of this Agreement and is effective until terminated as provided herein ("Term"). Each Statement of Work issued hereunder becomes effective as of the effective date specified in the Statement of Work and continues for the Term specified in the Statement of Work, unless terminated earlier as provided herein. Company Affiliates may enter into Statements of Work with Service Provider under the terms of this Agreement. The references to Company for purposes of this Section, applies to any Company Affiliate which has entered into a separate Statement of Work with Service Provider, except that a Company Affiliate alone shall not have the authority to terminate this Agreement as to Company or any other Company Affiliates, and the Company Affiliate, and not Company, is the responsible party for the Statement of Work. Notwithstanding anything in this Agreement to the contrary, Company shall have the option of terminating one or more Statements of Work without terminating this Agreement or any other Statements of Work.

9.2 **Termination for Convenience.**

(a) **Termination of Agreement.** Company or Service Provider may in its sole discretion terminate this Agreement without cause and for convenience by giving the other party at least ninety (90) business days' prior written notice of the termination; provided, however, that this Agreement shall continue to remain in effect with respect to any Statement of Work(s) outstanding as of the date of such termination, until such Statement of Work(s) are themselves either completed or terminated.

(b) **Suspension or Termination of Statement of Work.** A Statement of Work may, if expressly so indicated, provide for its own term and termination, but such termination in and of itself will not terminate this Agreement. Any Statement of Work may be suspended or terminated in whole or in part upon written notice from Company, with or without cause. Upon receipt of notice of suspension or termination, Service Provider shall inform Company of the extent to which performance has been completed through such date, and collect and deliver to Company (or otherwise as Company may reasonably request) whatever Deliverables then exist in a manner reasonably prescribed by Company in accordance with this Agreement. Service Provider shall be paid for all Deliverables of Service Provider that conform to the Specifications or otherwise meet this Agreement's requirements through the date of suspension or termination, provided that such payment shall not be greater than the payment that would have become due if the work had been completed. Service Provider may not suspend or terminate any Statement of Work once Service Provider has begun performance of the Services.

9.3 **Termination for Cause.**

(a) **Material Default.** If either party materially defaults in the performance of any of its obligations under this Agreement or any Statement of Work, the non-defaulting party may immediately terminate this Agreement and all outstanding Statements of Work as of a date specified in such notice of termination. For purposes hereof, a party shall be deemed to be in material default if it: (a) materially breaches any of its duties, obligations or responsibilities under this Agreement or a Statement of Work which default is not

10. **INSURANCE**

10.1 **Coverage Amounts.** Without limiting Service Provider's undertaking to defend, indemnify and hold Company harmless as set forth herein, Service Provider shall obtain and maintain insurance with the following coverages and terms:

- (a) Commercial General Liability coverage, including contractual liability for all written contracts, personal injury liability and completed operations coverage with \$2,000,000 combined single limit of liability for each occurrence and in the aggregate for bodily injury and property damage.
- (b) Professional or Errors and Omissions Insurance providing liability coverage for the professional services to be performed under this Agreement with \$10,000,000 limits of liability for any one claim made.
- (c) Workers compensation insurance with statutory limits covering Service Provider's workforce, affording protection in any state in which Service Provider's workforce may operate, including Employer's liability insurance with \$1,000,000 limits of liability; alternate employers endorsement to workers compensation policy.
- (d) Business automobile liability covering all owned, non-owned hired autos and autos owned or borrowed by workers or contractors while used in the course of their employment with \$1,000,000 limits of liability for bodily injury and property damage arising out of any one accident.
- (e) Excess or Umbrella Liability coverage with a minimum limit of four million dollars (\$4,000,000) coverage in excess of the coverage as set forth in items 10.1 above
- (f) Commercial Blanket Employee Fidelity Insurance providing \$1,000,000 limits of primary coverage for all Service Provider's workers and all of its contractors or subcontractors of every tier, including legal liability coverage for loss of Company's money, securities or property through fraudulent or dishonest acts.

10.2 **Insurance Company Ratings.** Service Provider shall provide insurance coverage by insurance companies having policy holder ratings no lower than "A" and financial ratings not lower than "VII" in the latest edition of Best's Insurance Guide in effect as of the date of this Agreement.

10.3 **Certificates of Insurance.**

- (a) **Provide to Company.** Service Provider shall immediately submit and, upon renewal of such insurance coverage, certificates of insurance to Company as evidence that the specified forms, endorsements and amounts of insurance as required are in force. All certificates shall include a clause obligating the insurer(s) to give the certificate holder not less than thirty (30) days prior written notice of any material change in, cancellation of, or intent not to renew the insurance.
- (b) **Requirements for Subcontractors.** Service Provider shall require similar insurance and maintain on file certificates of insurance from its Subcontractors of every tier, providing copies of certificates to Company upon reasonable request.

10.4 **No Restriction.** The insurance policies listed above are restricted by the country or state in which any Services are being performed. In the case of Services performed outside the United States where insurance is required by law, the insurance must be placed with a company admitted to do business in that country.

10.5 **Primary Coverage.** The foregoing insurance coverage is primary and non-contributing with respect to any other insurance or self-insurance that may be maintained by Company and its Affiliates and shall contain a cross-liability or severability-of-interest clause.

10.6 **Inclusion of Company and its Affiliates.** Company and its Affiliates shall be specifically included as an additional insured under the following coverage, if required: commercial general liability, commercial automobile/trucker's coverage/motor carrier coverage, and umbrella/excess liability coverage, for liability or loss arising out of or in any way associated with any act, error, omission or product of Service Provider, its directors, officers, shareholders, its workforce or anyone else for whose acts or products Service Provider may be held responsible (with coverage to Company at least as broad as that which is provided to Service Provider and not lessened or avoided by endorsement).

10.7 **Deductibles.** All deductibles or self-insured retentions are the sole responsibility of Service Provider.

10.8 **Term for Insurance.** All liability insurance requirements shall remain in effect for 2 years after termination of this Agreement.

10.9 **Service Provider's Separate Insurance Obligations.** The insurance obligations imposed by this Section are separate and distinct from any indemnification obligations imposed by this Agreement. Service Provider agrees that carrying insurance as required in this Agreement shall in no manner lessens nor affects Service Provider's other obligations or liabilities set forth in this Agreement, including without limitation any indemnification obligation.

11. **GENERAL**

11.1 **Assignment.** Each party agrees it will not to assign this Agreement without the other party's prior written consent (which consent shall not be unreasonably withheld), and that any attempt to do so is void and has no effect. All such assignments (except to the extent that this Agreement expressly provides otherwise) are prohibited.

11.2 **Binding Effect.** This Agreement will be binding upon and inure to the benefit of the parties hereto and their respective successors and permitted assigns.

11.3 **Governing Law.** The substantive and procedural laws of the State of Delaware (without giving effect to its conflicts of law principles and without regard to the Uniform Computer Information Transactions Act ("UCITA") or any version or revision of UCITA govern all matters arising out of or relating to this Agreement or any Statement of Work, including, without limitation, its validity, interpretation, construction, performance and enforcement. The provisions of the United Nations Convention on Contracts for the International Sale of Goods do not apply to this Agreement or to any Statement of Work.

11.4 **Venue.** The parties consent to the exclusive jurisdiction of, and venue in, any federal or state court of competent jurisdiction located in Federal Court in Delaware for the purposes of adjudicating any matter arising out of or relating to this Agreement or any Statement of Work.

11.5 **Notices.** All notices required to be given to a party under this Agreement are to be delivered to the following addresses, or any other addresses designated by the parties by notices delivered in accordance with this Section:

If to Service Provider: Examination Management Services, Inc.
3050 Regent Boulevard, Suite 400
Irving, Texas 75063
Attn: General Counsel

If to Company: Transamerica Procurement MS: 1130
4333 Edgewood Rd NE
Cedar Rapids, IA 52499

With a separately delivered copy to:
General Counsel
Money Services, Inc.
4333 Edgewood Rd NE
Cedar Rapids, Iowa 52499

Any notice required or permitted under this Agreement is to be given in writing and is deemed effectively given: (a) upon personal delivery to the party to be notified; (b) upon confirmation of receipt by fax by the party to be notified; or (c) deposit with a reputable overnight courier, prepaid for overnight delivery and addressed as set forth in this Section and upon confirmation of delivery to recipient.

11.6 **No Waiver.** The failure of a party to enforce any provision, exercise a right or pursue a default of this Agreement shall not be considered a waiver of its rights. The express waiver of a provision will be effective only in the specific instance, and as to the specific purpose, for which it was given. Unless stated otherwise, all remedies

provided for in this Agreement are to be cumulative and in addition to, and not in lieu of, any other remedies available to either party at law, in equity or otherwise.

11.7 **Severability.** Any part or provision of this Agreement that is held to be inoperative, unenforceable, voidable or invalid in any jurisdiction shall, as to that jurisdiction, be inoperative, unenforceable, void or invalid without affecting the remaining provisions in that jurisdiction or the operation, enforceability, or validity of that part or provision or any other provision in any other jurisdiction, and to this end, the provisions of this Agreement are declared to be severable. Should any part or provision of this Agreement be held inoperative, unenforceable, voidable or invalid in any jurisdiction, such part or provision shall, as to that jurisdiction, be replaced with a provision that accomplishes, to the extent possible and lawful, the original business purpose and economic intent of such part or provision in a valid and enforceable manner, and the remainder of this Agreement shall remain effective and binding upon the parties hereto. In the event the ruling and/or the controlling principle of law or equity leading to the holding is subsequently overruled, modified, or amended by legislative, judicial, or administrative action, the part or provision(s) in question as originally set forth in this Agreement shall be deemed valid and enforceable to the maximum extent permitted by the new controlling principle of law or equity.

11.8 **Effect of Headings.** The section headings contained in this Agreement are for convenience only and do not affect the construction or interpretation of any provision of this Agreement.

11.9 **Authorship/Fees and Expenses.** This Agreement is the result of arm's length negotiations between the parties and each of the parties has agreed to the use of the particular language in this Agreement. The parties further acknowledge that any questions of doubtful or unclear interpretation are not to be resolved by any rule or interpretation against the drafters, and that each party has participated in drafting this Agreement. Accordingly, this Agreement is to be construed without regard to the party or parties responsible for its drafting or preparation. Except as expressly provided in this Agreement, each party hereto shall be responsible for all fees, costs and expenses incurred by that party in connection with the preparation of and performance under this Agreement.

11.10 **Force Majeure.** Neither party is to be liable to the other party for any failure or delay caused by Force Majeure. The date of performance for the nonperforming party shall be extended for a period equal to the time lost by reason of any delay arising directly from any Force Majeure event, provided however that if the Force Majeure event lasts more than thirty (30) business days, Company has the right to immediately terminate this Agreement with no further obligations to Service Provider.

11.11 **Counterparts.** This Agreement may be executed in counterparts and delivered to each of the parties by facsimile. Facsimile or PDF signatures are deemed as legally enforceable as the original. Each such counterpart is deemed an original instrument, but all such counterparts taken together constitute one and the same agreement.

11.12 **Survival.** Upon termination of this Agreement for any reason, any section that by its nature should survive this Agreement to be effective shall survive and continue in full force and effect and be binding upon the parties, including, without limitation, Sections 4, 5, 6, 7, 8, 9.4, 9.5, 10 and 11.

11.13 **Business Forms Terms and Conditions.** If the terms and conditions in any purchase order or sales order, invoice, quote form or any other business form conflict with this Agreement, the terms and conditions contained in this Agreement are controlling.

11.14. **No Solicitation.** Each party agrees that during the term of this Agreement and for a period of one (1) year after the termination of this Agreement, it will not, except as part of an advertisement of employment opportunities in a publication of general circulation: (i) hire any person who is at any time during the term of this Agreement an employee of the other party or an Affiliate of the other party; (ii) directly solicit, entice, induce or encourage any person who is at any time during the term of this Agreement an employee of the other party or an Affiliate of the other party; or (iii) directly approach any such employee of the other party or an Affiliate of the other party for such purpose or authorize or knowingly approve the taking of such actions by any other person, corporation or entity, in each case without the express written consent of the employee's employer, which consent may be withheld in the sole and absolute discretion of the employer. The provisions of this Section shall survive termination of this Agreement as necessary to affect its purpose. Notwithstanding the foregoing, the above limitation does not apply in

the event an employee of either party or of an Affiliate has independently submitted his or her resume to an employment agency or recruiter, and such employment agency or recruiter forwards such resume or other information on to either party.

11.15. **Examination Rights.** Company shall have the right upon not less than fifteen (15) business days prior written notice, to examine and copy applicable records and practices of the Service Provider for the purpose of confirming compliance with the terms of this Agreement and of any Statement of Work. Such right shall be exercised no more than once annually during normal business hours and in a manner that does not unreasonably interfere with the business operations of the Service Provider. If the examination discloses an overpayment of any amount due by Company under this Agreement by more than ten percent (10%), Service Provider shall reimburse Company's reasonable expenses of examination.

11.16 **Regulatory Compliance and Assurances**

- (a) During the Term of this Agreement, Service Provider shall perform its obligations herein in such a manner as to be in full compliance with all applicable Federal and state regulations. Service Provider shall provide Company with all data and reports necessary for Company to comply with all Federal and state regulations applicable to the Services provided by Service Provider.
- (b) Provided that such enactments or regulations do not prohibit Service Provider from performing the Services for Company, Service Provider shall use commercially reasonable efforts to perform the Services regardless of changes in legislative enactments or regulatory requirements. If such changes prevent Service Provider from performing its obligations under this Agreement, Service Provider shall, when appropriate, make commercially reasonable efforts to develop and implement a suitable temporary work around until such time as Service Provider can perform its obligations under this Agreement without such temporary work around.
- (c) Service Provider and Company acknowledge and agree that the performance of the Services will be subject to regulation and examination by Company's regulatory agencies to the same extent as if such Services were being performed by Company. Upon reasonable request, Service Provider agrees to provide any appropriate assurances to such agency and agrees to subject itself to any appropriate examination or regulation.

11.17 **Foreign Corrupt Practices Act.** Service Provider shall not violate, or cause Company to violate the United States Foreign Corrupt Practices Act or any other similar applicable anticorruption laws or regulations ("FCPA") in connection with the Services and has not, and agrees that it shall not, in connection with the transactions contemplated by the Agreement, or in connection with any other business transactions involving Company or any Company Affiliate pay, offer, promise, or authorize the payment or transfer of anything of value, directly or indirectly to any government official or employee (including employees of government owned or controlled companies or public international organizations) or to any political party, party official, or candidate for public office, or any other person or entity, if such payments or transfers would violate the laws of the country in which made or the laws of the United States.

It is the intent of the parties that no payments or transfers of value by Company or Service Provider in connection with this Agreement shall be made which have the purpose or effect of public or commercial bribery, or acceptance of or acquiescence in, extortion, kickbacks, or other unlawful or improper means of obtaining business.

11.18 **Entire Agreement.** This Agreement, including all Statements of Work, schedules, amendments, appendices and other attachments, constitutes the complete and exclusive statement of the agreement between Service Provider and Company and supersedes all prior oral or written proposals, prior agreements and other prior communications between the parties, concerning the subject matter of this Agreement, except for prior provisions regarding confidentiality and nondisclosure. No amendment, waiver or modification of this Agreement is binding unless it is in a writing that explicitly references this Agreement and is signed by authorized representatives of both parties.

IN WITNESS WHEREOF, the parties have entered into this Agreement as of the Effective Date. Each signatory to this Agreement represents and warrants that he or she possesses all necessary capacity and authority to duly execute and deliver this Agreement on behalf of the entity for which such person is signing.

Company

MONEY SERVICES, INC.

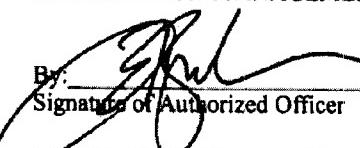
By: 

Signature of Authorized Officer

Bob Plaza, Vice President
Printed Name and Title

Service Provider

EXAMINATION MANAGEMENT SERVICES, INC.

By: 

Signature of Authorized Officer

Robert P. Brook, Executive Vice President and CDO
Printed Name and Title

EXHIBIT A

TEMPLETE

MONEY SERVICES, INC.

STATEMENT OF WORK

IN WITNESS WHEREOF, the parties have entered into this Statement of Work as of the date written above.

Company

MONEY SERVICES, INC.

By:

Signature of Authorized Officer

Printed Name and Title

Service Provider

EXAMINATION MANAGEMENT SERVICES, INC.

By:

Signature of Authorized Officer

Robert P. Brook, Executive Vice President & CDO

Printed Name and Title

**INFORMATION SECURITY
EXHIBIT B**

1. **Overview.** The purpose of this Attachment is to define the Information Security practices that Service Provider is required to establish, administer and maintain to protect Company Information Assets.
2. **Policy.** It is Company's policy that the following Information Security practices be established, administered and maintained by any third party having access to Company Information Assets, without exception.
3. **Definitions for purposes of the Information Security Requirements Exhibit B.**
 - a. "Agent" means anyone who, through either an agency or contractual relationship, has authority to view, host, store, process, transmit, print, back-up or destroy Company Information Assets.
 - b. "Agreement" means the contract entered into between the Company and the Service Provider, and to which this document is attached as an Attachment.
 - c. "Company Information Assets" are Information Assets belonging to or under the control of Company, including without limitation, all information and data provided by Company to Service Provider in any form, and any information or data generated as a result thereof (excluding any information that is properly of public record or that Company provides written permission for its disclosure).
 - d. "Information Assets" are defined as information and data in any form, whether electronic, hardcopy, photographic image, microfiche or microfilm or in digital, magnetic, optical or electronic form. It also includes all computing, network, and telecommunications systems and equipment which view, host, store, process, transmit, print, back-up or destroy information and data (e.g. personal computers, laptops, workstations, servers, network devices, software, portable storage devices, electronic storage media, cabling, and other computing and infrastructure equipment).
 - e. "Information Security" is defined as the protection against the loss of Information Assets' confidentiality, integrity and availability.
 - f. "Information Security Breach" is defined as any unauthorized act that bypasses or contravenes Company's information security measures as defined herein. It also encompasses the unauthorized use or disclosure of, or unauthorized access to or acquisition of, Company Information Assets.
 - g. "Information Security Program" is defined as the collection of policies, standards, procedures and controls, taken as a whole and implemented by Company or Service Provider, that are designed to protect the confidentiality, integrity, and availability of Information Assets.
 - h. "Information Security Vulnerability" is defined as a weakness in information security controls which could be exploited to gain unauthorized access to Company Information Assets.
 - i. "Physical Security" or "Physically Secured" is defined as the protection of information in hardcopy form against loss or unauthorized acquisition, access or disclosure during its production, storage, distribution, use or destruction. It also encompasses the protection of information technology hardware, infrastructure and facilities, as well as power or environmental control utilities used in data processing operations to protect against damage, destruction, or misuse of Information Assets.
4. **Organizational Roles and Responsibilities.** Service Provider organizational roles and responsibilities must include a chief information security officer, or comparable role assigned to one of Service Provider's officers or

senior management, to be responsible for the establishment, administration, and maintenance of a comprehensive written Information Security Program. The Information Security Program must include, at a minimum, the practices described in this Attachment.

5. **Non-Disclosure of Company Information Assets.** Service Provider acknowledges that the unauthorized release or misuse of the Information Assets could cause harm to the business reputation of either or both Service Provider and Company. Service Provider will not, and will cause its employees and Agents engaged in providing services to Company to not, knowingly take any action or omission which would result in the unauthorized release or misuse of the Information Assets of Company. Any actual or suspected Information Security Breach experienced by Service Provider involving Company Information Assets, must be reported by Service Provider to Company within forty-eight (48) hours of its detection.
6. **Information Security Framework and Right to Audit.**
 - a. The Service Provider's Information Security Program shall conform to the framework set forth by the International Standards Organization in a standards document entitled "Code of practice for information security management" (ISO/IEC 27002:2005, and as may be amended from time to time.). In addition to the standards outlined therein, Service Provider's Information Security Program must include the practices described in this Attachment. Service Provider's Information Security Program must be reviewed annually or whenever there is a material change in business practices that may implicate the security posture.
 - b. At Company's expense, promptly upon receipt of Company's written request, Service Provider shall grant Company, or a third party on Company's behalf, permission to perform an audit or assessment of Service Provider's compliance with the Information Security Program requirements at least annually. Following any Information Security Breach of Service Provider involving Company Information Assets such audit will be done at Service Provider's expense. The audits or assessments may be written or physical or as otherwise determined by Company. At Company's request at any time during the term of this Agreement, Service Provider agrees to certify in writing to Company Service Provider's compliance with the terms of this Attachment.
 - c. Service Provider, promptly upon receipt of Company's written request shall (a) provide to Company a report expressing the opinion of an independent third-party who, at the time of the review, holds current certifications as both a Certified Information Systems Auditor (CISA) from the Information Systems Audit and Control Association (ISACA) and a Certified Information Systems Security Professional (CISSP) from the International Information Systems Security Certification Consortium ("(ISC)2") on the effectiveness of Service Provider's information security controls; or (b) respond to any reasonable Company requests for information regarding Service Provider's information security program and practices. This request can be no more than annually unless there has been a change in ownership of the Service Provider or an Information Security Breach involving Service Provider.
 - d. Promptly upon receipt of Company's written request, Company may audit Service Provider Business Continuity Plan (BCP) and Disaster Recovery (DR) materials which pertain to or affect Company Information Assets, including BCP and DR plans and test results, at least annually, and following any man-made or natural disaster.
 - e. Service Provider attests that software and services provided under the Agreement, if any:
 - i. Does not contain undocumented features;
 - ii. Does not contain hidden mechanisms that could be used to compromise Company Information Assets;

- iii. Will not compromise, require modification of, disable or otherwise circumvent previously implemented information security controls.

7. General Information Security Requirements.

- a. Service Provider must ensure appropriate segregation of duties exist for all job functions and roles performed by its employees and Agents to ensure that no individual, within or external to Service Provider's organization, has conflicting duties that could jeopardize Company Information Assets.
- b. Company Information Assets should not be divulged in any way to anyone without a specific valid business "need to know" and Company written authorization.
- c. Access to all Company Information Assets must:
 - i. adhere to the principle of "least privilege," ensuring that only the most minimal level of access needed for a given job function of access is granted to Service Provider's employees and its Agents;
 - ii. be restricted to only authorized personnel who have a specific business "need to know."
- d. Computer services employed to view, host, store, process, transmit, print, back-up or destroy Company Information Assets must adhere to the principle of "least privilege," ensuring that only the most minimal level of access needed to perform processing is granted to these computer services.
- e. Hardware and software owned by Service Provider personnel must not be allowed to connect to or interact with the Company's company network without:
 - i. an appropriately scoped risk assessment, including the identification of existing and compensating controls based upon the requirements within this Attachment;
 - ii. verification of the implementation of controls identified within the risk assessment;
 - iii. obtained approvals of Company IT Network Management and the appropriate Chief Information Officer of the enterprise or division of Company involved.
- f. Service Provider's users should not be allowed to install their own personal software on Service Provider Information Assets.
- g. Service Provider portable devices that store, process, transmit or destroy Company Information Assets, such as laptops, personal digital assistants (PDAs), Blackberries[®], smart phones, hand-held or palmtop computers, portable memory drives, and other similar portable devices must be configured to make use of industry standard encryption technology that fully protects these devices' storage and transmission capabilities from unauthorized access.

8. Information Asset Classification and Management. Service Provider must classify and control its Information Assets to indicate the ownership, custodianship, and degree of sensitivity consistent with Company's Information Asset classification in order to ensure that Company Information Assets receive an appropriate level of protection by Service Provider. The inventory of Service Provider's Information Asset classification repository must be maintained and kept current. Recommended classifications are as follows:

- a. Non-sensitive Business Data and Public Information Assets (Public Release)
 - i. "Non-sensitive Business Data" refers to all Information Assets determined by Company to not be sensitive or confidential as defined below;

- ii. "Public Information" refers to all Information Assets that comes from public sources or is provided by Company to the general public; examples include periodicals, public bulletins, published company information, published press releases, etc.
- b. Confidential and Proprietary Company Information Assets (Confidential)
 - i. "Confidential" or "Proprietary Information Assets" refers to Information Assets that are internal to Company, though it may be shared with Service Provider under the terms of the Agreement, and are not considered by Company to be Public Release; examples include unpublished corporate financial information, information about impending mergers and acquisitions, dormant account information, marketing plans, passwords and encryption keys, employee and customer non-public personal information (such as personally identifiable information, personal financial information or personal protected health information), product designs, customer records and correspondence, and other information or data which if disclosed without appropriate authorization could result in a competitive disadvantage or liability or loss to the Company.
 - c. Record retention periods that meet federal and state retention requirements must be established and maintained by Service Provider. In addition, the Parties may agree in writing to specific retention requirements that Service Provider will follow, including but not limited to, retention for compliance, litigation, legal or regulatory purposes.
 - d. Destruction of Company Information Assets must not occur outside of the agreed upon retention schedule without authorization from Company management. The destruction methodologies must be performed in a secure manner such that the information cannot be read or re-created after disposal. Service Provider is encouraged to adhere to the guidelines provided by the National Association for Information Destruction (NAID), which can be found at <http://www.naidonline.org>. Service Provider must also take into consideration the impact of disposal on the environment.
 - e. At Company's expense, promptly upon receipt of Company's written request, Service Provider will work with Company to return all Company Information Assets in a reasonable manner and timeframe, taking into consideration then current technologies and industry best practices for information transfer and asset transportation, ensuring at a minimum that the information is either destroyed according to Company requirements or returned to Company in a format that is reasonably organized and usable by Company. However, if such return is infeasible, Service Provider will limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible and extend the provisions of this agreement as long as the information is maintained. Where errors in data transfer exist, Service Provider agrees to work with the Company to provide reasonable effort to correct problems with the integrity of transferred data.
- 9. **Human Resources Management.** The following administrative requirements must be implemented by Service Provider where Company Information Assets are stored, processed, transmitted, or destroyed; except as may be otherwise required for compliance, litigation or legal or regulatory purposes.
 - a. Service Provider employees and Agents must be subject to a sufficient criminal background check prior to employment to ensure people with a criminal history do not have access to Company Information Assets. The Service Provider agrees it will provide no employees or Agents who have been convicted of a felony involving theft, dishonesty, or breach of trust, or any other crime that disqualifies someone from working in the business of insurance as set forth in the Federal Crime Bill. Further, Service Provider will conduct a background check on each employee or Agent that is sufficient to screen out those who have been convicted of crimes involving behavior that, if it occurred on the Company's site, could result in injury to people or impairment of assets.

- b. Service Provider must follow a documented method or procedure that governs the creation, suspension, cancellation, modification, and deletion of user accounts for its employees and Agents. These methods or procedures must include, at a minimum, the following:
 - i. Employees and Agents with valid user accounts must have their user accounts disabled immediately upon termination of employment or business engagement;
 - ii. Employees and Agents who experience an absence longer than ninety (90) days must have their user accounts disabled. These user accounts may be re-enabled upon their return to work; otherwise, these accounts shall be deleted upon termination of the Employee or Agent;
 - iii. Employees and Agents whose job responsibilities change must have their access levels reviewed to determine if changes need to be made in order to ensure they do not have access to Information Assets for which they do not have a specific business need.
- c. During employment or when under contract:
 - i. Service Provider must include Information Security requirements within job descriptions or other written documentation for Service Provider employees and Agents whose job roles will have access to Company Information Assets;
 - ii. Service Provider must maintain an Information Security awareness and training program for its employees and Agents to ensure the employees and Agents are aware of their responsibility to protect and maintain the confidentiality and security of Service Provider and Company Information Assets;
 - iii. Service Provider shall impose disciplinary measures for violations of its Information Security Program.
- d. Upon termination of employment or contract:
 - i. Service Provider shall notify Company in writing within 24 hours when Service Provider's employees and Agents who have access to Company's network and internal systems are reassigned and no longer need access, or are no longer working for Service Provider, thereby enabling Company to remove access in a timely manner;
 - ii. Service Providers must secure all Company Information Assets within their custody from employees and Agents upon termination of employment or contract.

11. Physical Security.

- a. Access to Company Confidential Information Assets must be controlled to protect the confidentiality, integrity, and availability of Company Confidential Information Assets with appropriate administrative, logical, and physical safeguards, including but not limited to:
 - i. locking office doors;
 - ii. securing storage containers; and
 - iii. shredding or otherwise securely destroying Information Assets at appropriate times.
- b. Physical entry to Service Provider's premises must be controlled such that unauthorized entry is prevented, detected and reported to appropriate Service Provider personnel immediately. All entry and exit points must be secured, logged and monitored to ensure only authorized personnel may gain entry to Service Provider's buildings and secured areas.

- c. Where Service Provider has utilized identification badges or similar tokens for its employees and Agents, a documented process must exist, along with supporting procedures, to ensure lost badges and tokens are disabled immediately upon notification of the loss.
- d. When a Service Provider employee or other Agent is terminated, procedures must exist to ensure the identification badges are immediately disabled.
- e. All Company Information Assets in Service Provider's possession must be physically secured in an access-controlled area, in a locked room, or secured storage container or file cabinet.
- f. Company Information Assets must not be removed from Service Provider's premises without written consent from Company and written authorization from Service Provider management.
- g. All Company Information Assets, together with Service Provider Information Assets used to provide services to Company, must be protected to minimize the risk of physical and environmental threats that could jeopardize Information Asset confidentiality, integrity, and availability.
- h. Physical access to computer sessions must be secured when a user who is actively logged into session is not physically present to monitor activity and viewing of Information Assets displayed within that session. Examples of physical controls include, but are not limited to:
 - i. utilizing screen savers which lock the screen and keyboard access after a short period of inactivity;
 - ii. manually locking the keyboard;
 - iii. physically securing the office where the computer resides;
 - iv. positioning the monitor away from an unauthorized view.
- i. **Information Back-up.**
 - i. Adequate backup facilities should be provided to support the recovery of Company Information Assets in accordance with Company disaster recovery requirements and record retention schedules. Minimal requirements include:
 - ii. Media containing back-up copies of Confidential and Proprietary Company Information Assets should be encrypted using industry standard methods to conceal these Information Assets from unauthorized access;
 - iii. The back-up storage media used to store Company Information Assets must be of a type that has been determined by Service Provider to be appropriate for the confidentiality and retention requirements of the data it will contain;
 - iv. As it is critical that the back-up storage media be machine readable in the event it is needed for restore and recovery operations, random controlled testing of the restoration process must occur;
 - v. Back-up copies of Company Information Assets, together with complete and accurate records of the back-up copies, must be stored at a physically secured offsite location as a measure of protection against total loss of Information Assets in the event of a system failure or disaster;
 - vi. Company Information Assets should be backed up on a schedule that aligns with disaster recovery requirements. This schedule includes requirements for weekly full backups, daily incremental backups, quarter end backups and year end backups;

vii. No more than one (1) full back-up and six (6) days of subsequent incremental back-ups may be stored on Service Provider premises at any time.

j. **Network Security.**

- i. Company may terminate any network or other Remote Connection with Service Provider at any time without warning if it is suspected or confirmed that any such connection is not secure.
- ii. Company Information Assets must not exist on any computer or device that is directly exposed to the Internet or other non-Service Provider network, unless specifically authorized by Company in writing.
- iii. Service Provider shall establish and maintain appropriate controls for its electronic interfaces and connections between its own systems and those of others (Remote Connections) utilizing industry best practices.
- iv. Devices must be verified prior to connecting to the Company or Service Provider network segments where Company Information Assets reside to comply with the following hardening requirements to protect from compromise:
- v. Devices must employ an antivirus and file integrity checking system with:
 1. A method for updating antivirus definition information to be current at all times;
 2. Enabled real-time antivirus scanning of system activity, including all accessed files and memory;
 3. Scheduled weekly full directory and file antivirus scan;
- vi. Devices must employ up-to-date system software, including but not limited to, up-to-date system software patches and security updates.
- vii. Devices must employ a firewall, proxy or other network traffic filtering technology to deny invalid in-bound traffic to and reasonably protect out-bound traffic from that device;
- viii. System logs or equivalent tracking software must be configured to reasonably capture common errors and invalid access attempts;
- ix. The integration of new software on devices granted connectivity permission must be preceded by a risk assessment and incorporate formal change control procedures to determine and protect the impact to the Company network.
- x. Permission to connect any device to the Company network shall be proceeded by:
 1. A Company risk assessment to determine the impact to the Company network;
 2. Approvals from Company, including its IT network manager, impacted technical IT managers, and a divisional Chief Information Officer or his/her designee; and
 3. Service Provider networks must have firewalls deployed at the network perimeter to deny unauthorized in-bound and appropriate out-bound network traffic from the Internet and other non-Service Provider networks.

- xiii. Service Provider applications and systems that view, host, store, process, transmit, print, back-up or destroy Company Information Assets must be logically segregated from other systems on the Service Provider internal network by an appropriate firewall- or proxy-based, or similar, architecture that will disallow unauthorized in-bound and out-bound connections to Company Information Assets.
- xiv. Intrusion detection systems (IDS) or intrusion prevention systems (IPS) must be in place to provide reasonable logging and protection against malicious network activity. These systems should be configured to alert appropriate information security and information technology personnel who will then bear the responsibility to take action to disallow said network activity from affecting Company Information Assets.
- xv. Unattended network ports must be secured or disabled when not in use. Where business requirements justify the need, network ports may remain active provided that Service Provider management has reviewed the business need and there is documented approval. Examples of such need would include network ports in conference rooms, shared work areas, etc.
- xvi. Wireless network access points must be configured to ensure that only authorized Service Provider devices may establish a connection to the Service Provider internal network where Company Information Assets are viewed, hosted, stored, processed, transmitted, printed, backed-up or destroyed. Further, the wireless network connections established must utilize industry best practices for encryption and other appropriate safeguards designed to protect against unauthorized access and use.

k. System Event Logging, Monitoring, and Reporting.

- i. Service Provider computer and network systems used to provide services to Company must log significant events including, but not limited to, the following:
- ii. Unauthorized attempts to access Service Provider network or Company Information Assets must be captured and securely logged in such a way to support error handling and forensic needs.
- iii. Logs must be configured or secured such that they cannot be viewed or altered by anyone without authorization, including those with administrative privileges, unless such access is also logged in a tamper-evident manner;
- iv. Logs of unsuccessful login attempts to network and unsuccessful access to Information Assets must be reviewed on a regular basis to detect and appropriately act upon anomalous and suspicious system access attempts;
- v. When suspicious or anomalous activity is detected during a review of the aforementioned logs, it should be reported as directed by approved event handling procedures aligning with Information Security Incident Response plans.

l. Logical Access.

- i. All computer-based information systems connected to any portion of the Service Provider network where Company Information Assets are located or processed must employ, at a minimum, the following requirements:
- ii. Service Provider shall grant access to each user on a personally identifiable unique user account;
- iii. Wherever technically possible, the password settings for each user account must be configured using the following minimal configuration:

1. Minimum of eight (8) characters in length and contain characters from at least three (3) of the following four (4) character types:
 - a. upper case alpha characters;
 - b. lower case alpha characters;
 - c. numeric characters;
 - d. special characters (e.g., !, \$, @, etc.).
2. Expiration of password must be minimally set as follows:
 - a. Set to automatically require password changes, at a maximum, every sixty (60) days, for user accounts and any system account where the setting will not hinder production processing;
 - b. If the automatic expiration of a system account would potentially cause the risk of interruption of production processing, password changes may occur manually with the following alternate controls in place:
 - (i) The system account is assigned a unique owner who is ultimately responsible for the disposition and usage of the account and password;
 - (ii) The system account is configured with advanced complex password creation rules (e.g., extended password length, hashing algorithms, etc.);
 - (iii) The system account is limited wherever possible to allow log on capabilities only to required computers and/or services;
 - (iv) The system account is changed manually at least once a year and upon turnover of staff at the earliest time available so as not to affect processing;
 - (v) The system account complies with all other requirements within this Attachment.
- iv. The password settings for each vendor-supplied default account must be changed and configured using the minimal configuration outlined in this 14. a. ii.
- v. Accounts with any access to Company Information Assets must be configured wherever technically possible to disallow login capability after a maximum of seven (7), unless otherwise required to be a lesser number (e.g., PCI, etc.), consecutive unsuccessful login attempts.
- vi. Stored password text must be stored in an encrypted form in the user identity database, and they must be rendered unreadable during transmission and storage (e.g., appropriately concealed within strongly restricted directories, etc.) if embedded within batch files, automatic login scripts, software macros, terminal function keys, on computers where access controls are otherwise disabled, or any location where unauthorized individuals might discover them.
- vii. Passwords must be changed immediately if it is discovered that they are disclosed to or discovered by unauthorized parties.
- viii. Service Provider systems must be configured wherever technically possible to disable user sessions after a reasonable period of inactivity, based upon business risk.
- ix. Additional and/or stronger logical access safeguards may be implemented by Service Provider at its discretion, so long as such additional controls do not neutralize nor negate the effectiveness of existing controls for Company Information Assets as outlined within this Attachment.

m. System Development.

- i. Application and system development must follow a defined and documented systems development life cycle (SDLC) methodology that includes a preliminary review of information security requirements to ensure, at a minimum, the following:
 - ii. Vulnerability testing must be performed to ensure common security weaknesses are detected and corrected prior to being implemented;
 - iii. There must be separate physical or logical environmental partitions separating development, test, staging and production environments;
 - iv. The use of data within non-production environments must adhere to the following at a minimum:
 1. Wherever possible, fictitious data based upon real data cases must be employed in test environments;
 2. If Company Information Assets are used, the same controls must exist as within the production environment;
 3. If Company Information Assets are used, it must be immediately removed from all non-production environments upon the completion of its use;
 4. Handling and destruction of sensitive non-production data and output must be treated as the same level of confidentiality as if it were production;
 - v. Logical access controls must be defined, tested and incorporated to ensure they work as designed and support the ability to restrict access to only those Company Information Assets required for Service Provider and Company business requirements, while also supporting the principle of least privilege;
 - vi. Segregation of duties must be incorporated into the design of applications and systems to prevent the ability of a single person to perform multiple functions that could lead to fraud, theft, or other illicit or unethical activity through the use of the functions of the applications and systems where Company Information Assets are stored, processed, transmitted, or destroyed;
 - vii. Web-based applications exposed to the Internet must ensure vulnerability testing is performed to ensure the most common vulnerability weaknesses based upon industry best practices are identified and remediated to prevent them from being exploited in a way that could lead to unauthorized access to or disclosure of Company Information Assets;
 - viii. A formal, documented change management process must be used when making changes to applications and systems that view, host, store, process, transmit, print, back-up or destroy Company Information Assets. This change management process must, at a minimum, include the following:
 1. Each change must be reviewed and approved by Company management. Changes to applications and systems must not be deployed into production environments by the same people who do the development and quality assurance of applications and systems;
 2. A record of all changes to applications and systems must be maintained that identifies:
 - a. a brief description of each change that was made;
 - b. who made each change;
 - c. test plans and results for each change;

- d. who approved each change;
- e. when each change was made.

n. Information Security Incident Response and Breach Notification.

- i. Service Provider must establish and maintain a documented Information Security Incident Response program (ISIRP) that includes, at a minimum, the following:
 - ii. Service Provider must define and document the roles and responsibilities of its ISIRP team members;
 - iii. Service Provider ISIRP team members must receive training at least annually to ensure they understand what to do during an Information Security event or incident;
 - iv. Service Provider must establish and maintain a documented set of procedures and notification requirements to follow that provides guidance to the ISIRP team when responding to an event or incident;
 - v. Procedures and other documentation must provide guidance to the ISIRP team regarding Information Security event and incident records. All relevant event and incident logs, along with any related notes of actions taken in response to these events and incidents, must be secured and retained, based upon an approved retention schedule;
 - vi. Any unmitigated Information Security Breach experienced by Service Provider prior to the execution of the Agreement must be disclosed to Company.
- vii. Any actual or suspected Information Security Breach experienced by Service Provider involving Company Information Assets must be reported to Company within forty-eight (48) of its detection. A formal communication plan for notification must be defined and documented between the parties. The parties agree to reasonably coordinate and cooperate with each other in investigating the suspected breach. Service Provider shall take immediate steps to remedy the Information Security Breach at Service Provider's expense in accordance with applicable privacy rights and laws. Service Provider shall reimburse Company for actual costs incurred in responding to and/or mitigating damages caused by an Information Security Breach. For purposes of the Service Provider's reimbursement obligation in the preceding sentence, Service Provider shall only be obligated to reimburse a reasonable amount of Company's costs based upon the nature of the Security Breach, the size of the Security Breach and the number of individuals impacted by the Security Breach.

o. Business Continuity.

- i. Business continuity recovery point objectives (RPO) and recovery time objectives (RTO) must be discussed with Company and agreed to commensurate with the execution of the Agreement. This is done to ensure Service Provider recovery capabilities and subsequent commitments to do so will meet Company's business requirements.
- ii. Service Provider or Agent shall maintain a documented business continuity and disaster recovery (BCP/DR) plan which, at a minimum, must:
 - ii. Govern and define the objectives and actions required during a BCP/DR event;
 - iii. Secure offsite copies of appropriate business continuity and disaster recovery documentation for retrieval in a reasonable time period by those who will need access to this information following a disaster event;

- iv. Define and document business continuity processes and procedures to enable Service Provider to perform the actions necessary to maintain critical business functions following a disaster event;
 - v. Define and document Information Asset disaster recovery procedures to enable Service Provider to recover Company Information Assets in a manner consistent with established and agreed upon RPO and RTO business continuity requirements;
 - vi. Prioritize recovery activity based upon a documented inventory of Company Information Assets in accordance with the established and agreed upon RPO and RTO;
 - vii. Define and document a formal communication plan to require that notification of any BCP/DR invocation be provided to Company within one (1) full business day of its occurrence.
- p. **Compliance.**
- i. Service Provider must comply with all applicable international, state, federal, and private industry regulatory and statutory requirements. Examples of some of these requirements include, but are not limited to, adherence to the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA).
 - ii. Unlicensed and/or unapproved software must not be used on any Company Information Asset or on Service Provider Information Assets.
 - iii. All software installed on Service Provider Information Assets must be approved by appropriate Service Provider management to ensure it satisfies a business need, configured to conform to the principle of "least privilege," and is in compliance with applicable technical and information security requirements.

EXHIBIT C
UNDERWRITING SERVICES

General Service Levels: Service Provider shall adhere to the following general requirements:

- * Company may allow transitional Service Levels for up to 3 months upon launch of new Service Provider to manage acclimation and adjustments.
 - Documents will be transmitted/provided in Company's standard image and data format, if applicable. If Service Provider cannot transmit images and data per Company's standard format request, then this Exhibit C will be amended to identify the mutually agreed-upon format for such transmissions.
 - Service Provider shall provide reporting to support adherence to applicable Service Levels as set forth in this Agreement, as well as on an ad hoc basis. Monthly reporting due by the 8th of each month for prior month's Service Level performance results.
 - Service Provider shall report Services received, canceled and completed on a monthly basis in accordance with the defined Service Levels within this Agreement in a format acceptable to all parties.
 - Service Provider will provide ad hoc reporting as needed or agreed upon.
 - Service Provider to provide a written Root Cause Analysis (RCA) & Remediation Plan by 10th day of month following failure to meet a Service Level Standard.
 - Service Provider will provide Company with copy (images) of Services within 2 business days of Services being completed.
 - Service Provider will maintain web sites linked to the Company's systems (when applicable), or external websites that provide both ordering and status functions. Service Provider will provide secured access including User ID's and Password management for Company employees as needed.
 - Service Provider will provide electronic ordering and status functions in data format as mutually agreed upon in writing.
 - Service Provider shall notify Company of any complaints received from customers of Company and/or Service Provider within 2 business days of notification. Additional historic or substantiating information needed for Company to assess complaint will be provided within 1 business day from Company's request.
 - Service Provider shall perform a quality assurance check a minimum of 5% of Services on a monthly basis. Results of the quality assurance check to be provided to the Company on a monthly basis for the prior month's quality results.

- Company reserves the right to audit Service Providers quality assurance process and results without cause upon ten (10) business days' notice. When requested, Service Provider will cooperate by providing information for Services selected by Company for such quality assurance reviews/audits.
- Service Provider shall discount specific line of Services by 5%, if not remedied for 3 consecutive months, for any month that Service Levels are not met which will be credited on the month following missed Service Levels. (For example, Service Level missed January, February and March, will cause 5% of the March invoice to be credited to Company's April invoice)
- Service Provider shall utilize only Company approved letters, e-mails and scripts when contacting Company's customers, applicants and/or producers.

Telephone Interviews (“Interview(s)”) - Service Provider shall perform the following Services, and shall meet or exceed Service Level Standards with respect to all Interviews:

- Contact the applicant by telephone as required by Company within twenty-four (24) hours of Company's request. Subsequent contacts should be at the rate of five (5) attempts in three (3) days should the Company provide new information / telephone number.
- Service Provider shall complete the Interview, which shall consist of mutually-agreed upon questions and reflex questions.
- The average service time (measured from the time and date the Service Provider receives Company's request to conduct the Interview until the time and date the Company receives the Interview, including all delays), computed on a monthly basis, will be five (5) or less business days, unless delayed by applicant or agent, 95% of the time; 100% of Interview requests will be delivered within 7 business days (unless scheduled over 7 days in advance or later date requested by applicant.)
- Service Provider shall remit completed Interviews to Company or otherwise notify Company that interview cannot be completed and the reason therefore.
- Interviews not completed within this time frame will remain open for a period of 45 days before being closed for billing; this is so that the applicant may call in to complete the interview without the need of placing a new order.
- Service Provider shall provide average length of interview on a semi-annual basis.

Face-to-Face or Paramedical Assessments (“Assessment(s)”) - Service Provider shall perform the following Services, and shall meet or exceed the following Service Level Standards with respect to all Assessments:

- Make appointment with the applicant for an Assessment at a reasonable hour as requested

by approved Company producers and/or by Company. Initial contact with the applicant will take place within two (2) business days of Company's request.

- Service Provider shall visibly display credentials during appointment and shall dress in a manner consistent with the professional service being completed.
- Service Provider shall ensure that all blood samples are kept cool and centrifuged within 4 hours of collection. All applicable fees for Services billed for applicants wherein fluid collection was handled improperly shall be deducted.
- Service Provider shall use best efforts to ensure that all medical information supplied by applicant has relevant details which include dates, diagnosis, outcome and any follow-up. Company may deduct 50% of all applicable fees for Services billed whereby relevant details are omitted by Service Provider.
- The average service time (measured from the time and date the Service Provider receives Company's request to conduct the Assessment until the time and date the Company receives the Assessment, including all delays), computed on a monthly basis, will be fourteen (14) or less calendar days 80% of the time; 90% of Assessment requests will be delivered within 28 calendar days (unless scheduled at a later date as requested by applicant.)
- Service Provider shall remit completed Assessment to Company or otherwise notify Company that assessment cannot be completed and the reason therefore.

Attending Physicians' Statements ("APS") - Service Provider shall perform the following Services, and shall meet or exceed the following Service Level Standards with respect to all APS:

- All APS requests will be accompanied by proper authorizations signed by the Company.
- Request, follow up, receive and forward copies of medical records from the physician, clinic or medical facility as requested by approved Company producers and/or from Company.
- 95% of all requests will have initial contact with the physician, clinic, or medical facility attempted no later than 1 business day following receipt of order; 99% of all requests will have initial contact with the physician, clinic, or medical facility attempted no later than 2 business days following receipt of order.
- Remit completed APS to Company or otherwise notify Company that APS cannot be completed and the reason therefore.
- Service Provider will report percentage of APS completed in > 14 calendar days, 21 calendar days, 28 calendar days and percentage completed over 28 calendar days.

- The average service time (measured from the time and date the Service Provider receives Company's request for APS until the time and date that Company receives the APS), computed on a monthly basis, will be fourteen (14) or less calendar days.
- No less than 65% completed within 14 calendar days. No less than 75% completed within 21 calendar days. And no less than 90% completed within 28 calendar days.

EXHIBIT D
Underwriting Services and Fees

Paramedical Services

Service Name	Service Codes	Price	Kit Cost	Kit Handling
Paramed Exam Only	2	\$42.75	NA	NA
Paramed, Blood and Urine	2+29	\$68.40	\$8.30	\$5.75
Paramed, ECG, Blood and Urine	2+123+29	\$96.90	\$8.30	\$5.75
Paramed and Blood	2+29	\$68.40	\$8.30	\$5.75
Paramed and EKG	2+123	\$71.25	NA	NA
Paramed and Urine	2	\$42.75	\$5.00	\$5.75
Paramed, DBS and Urine	2+5084	\$68.40	\$8.30	\$5.75
Paramed, EKG and Urine	2+123	\$71.25	\$5.00	\$5.75
Medical Exam Only	1	\$85.50	NA	NA
Medical, Blood and Urine	1+61	\$129.20	\$8.30	\$5.75
Medical, EKG, Blood and Urine	1+14+61	\$161.50	\$8.30	\$5.75
Medical, Blood, Urine and Treadmill	1+31+61	\$570.00	\$8.30	\$5.75
Medical and EKG	1+14	\$117.80	NA	NA
Medical and Treadmill	1+31	\$526.30	NA	NA
2 Urine collections on different days	283	\$70.30	\$10.00	\$5.75
Blood Draw and EKG	1198	\$71.25	\$8.30	\$5.75
Blood Draw Only	1018	\$42.75	\$8.30	\$5.75
Blood Draw with Stats (HT, WT, BP, Pulse)	1120	\$50.00	\$8.30	\$5.75
Urine Only (includes Recheck)	15	\$36.10	\$5.00	\$5.75
DBS Collection Only	5085	\$38.00	\$8.30	\$5.75
EKG Only	4	\$54.15	NA	NA
EKG with Blood, Urine and Stats (HT, WT, BP, Pulse)	1120+123	\$78.50	\$8.30	\$5.75
Oral Fluid Only	409	\$36.10	\$7.70	\$5.75
Blood Pressure Only	156	\$34.75	NA	NA
Blood Pressure Readings on 2 consecutive days	5	\$69.65	NA	NA
Physical Measurements (HT, WT, BP, Pulse)	23	\$34.20	NA	NA
Weight and Height Recheck	23	\$34.20	NA	NA
IGO Mobile	6000	\$11.50	NA	NA
Packet Take out	490	\$7.70	NA	NA
Cancellation Refusal at Door	19	\$23.75	NA	NA

Average Price of Gas Per Gallon	Surcharge
\$2.74 or less	\$0
\$2.75 - \$3.24	\$1.50
\$3.25 - \$3.74	\$2.00
\$3.75 - \$4.24	\$2.50
Above \$4.25	TBD

When the price of gas exceeds \$2.75 per gallon
Company will pay a fuel surcharge. 100% of this fuel
surcharge is allocated back to the examiner to defray
their fuel cost.

Rate Exceptions

Hawaii, Puerto Rico, Alaska and Guam 2 times above rate.
New York City, Nassau and Suffolk Counties, Boston, District of Columbia, California and Chicago 1.25 times above rate.

Medical Records

Service	2014 Price
APS Flat Rate*	\$50.00
Cancel/No Records	\$15.00
Rush Handling	\$10.00
Special Handling	Included

* The \$50.00 flat fee is to cover facility fees up to \$100.00. Fees in excess of \$100.00 require Home Office approval.

If fee approval is given, billed amount will be equal to the flat fee (\$50.00) plus the amount over \$100.00.

Interviews

Script Name	Report	Report Number	Rate Standalone	Rate w/report
PHI FE (old 45& over)	FR	1	\$22.35	n/a
PHI SR (old Final Expense 44&under)	FR	2	\$30.40	n/a
Transamerica Health Interview	FR	3	\$25.70	n/a
PHI-SI	FR	4	\$12.40	n/a
MedSup	FR	5	\$24.70	n/a
Juvenile	FR	6	\$18.10	n/a
LTC	FR	TBD	\$23.75	n/a
Agent Quality	QN	1	\$8.00	\$2.75
Disability Questionnaire	QN	2	\$8.00	\$5.25

Script Name	Report	Report Number	Rate Standalone	Rate w/report
Anemia Questionnaire	QN	5	\$8.00	\$6.25
Arthritis Questionnaire	QN	6	\$8.75	\$7.00
Back and Neck Pain Questionnaire	QN	7	\$10.25	\$8.00
Cancer Questionnaire	QN	8	\$8.25	\$6.25
Cerebral Palsy Questionnaire	QN	9	\$8.00	\$3.25
Diabetes Questionnaire	QN	10	\$10.25	\$8.00
Depression, Mental & Nervous Disorder	QN	11	\$10.75	\$8.50
Gastrointestinal Questionnaire	QN	12	\$8.75	\$7.00
Heart Disease/Disorder Questionnaire	QN	13	\$9.50	\$7.50
Heart Murmur Questionnaire	QN	14	\$8.00	\$5.75
Hepatitis Questionnaire	QN	15	\$11.50	\$9.00
Hysterectomy	QN	16	\$8.00	\$4.25
High Blood Pressure Questionnaire	QN	17	\$8.25	\$6.25
Lupus Questionnaire	QN	18	\$8.00	\$5.75
Multiple Sclerosis Questionnaire	QN	19	\$8.75	\$7.00
Pregnancy	QN	20	\$8.00	\$4.25
Respiratory Disorder Questionnaire	QN	21	\$8.25	\$6.25
Seizure Questionnaire	QN	22	\$10.75	\$8.50
Skin Cancer Questionnaire	QN	23	\$8.00	\$5.75
Sleep Apnea Questionnaire	QN	24	\$8.75	\$7.00
Stroke Questionnaire	QN	25	\$9.50	\$7.50
Thyroid Questionnaire	QN	26	\$8.00	\$5.25
Ulcer Questionnaire	QN	27	\$8.00	\$5.25
Occupation and Income	QN	28	\$8.00	\$4.75
Foreign Travel	QN	29	\$8.00	\$1.75
Military	QN	30	\$10.75	\$8.50
Tobacco Questionnaire	QN	31	\$8.00	\$1.05
Alcohol-Drug Questionnaire	QN	32	\$8.00	\$5.75
Driving Questionnaire	QN	33	\$8.00	\$4.25
Aviation	QN	34	\$14.25	\$11.00
Avocation	QN	35	\$11.50	\$9.00
NY Avocation	QN	36	\$11.50	\$9.00
MD Avocation	QN	37	\$10.75	\$8.50
FL Avocation	QN	38	\$10.75	\$8.50
Residency	QN	40	\$8.00	\$4.75
Close out/Cancellation	N/A	N/A	\$5.40	N/A
Language Line	N/A	N/A	Varies	N/A
Additional SI Questions	SR	99	See Note	N/A
Special Instructions Questions Only	SR	99	\$8.00	NA

Script Name	Report	Report Number	Rate Standalone	Rate w/report
General Medical Follow Up Questions**	QN	4	n/a	\$3.25

*Used by Company for specific questions. Max. 3 questions.

** This will only bill when a medical question is answered "Yes" in the 10 Year Medical HX section.

Inspection Reports

Service	2014 Price
Quick E-Search	\$12.20
Amplified with Source	\$40.05
Bus Amp w/Source	\$53.05
Business Beneficiary	\$34.80
Credit Report	\$10.25
Bankruptcy	\$10.25
Criminal Records*	\$23.30
*Criminal records have a fee assessed by the county that may apply as a pass thru fee	Varies
^Close Out - Includes cancellation/close out fee plus credit report	\$15.00
Language Line	Varies

[^]The credit report is ordered upon receipt. All close outs will include credit report since it is ordered prior to interview

STATEMENT OF WORK

This **STATEMENT OF WORK** ("SOW") is made effective on the 12th day of October, 2017 ("Effective Date"), by and between Examination Management Services, Inc. ("Consultant") and Money Services, Inc. ("MSI"). All the terms, conditions, specifications, and other provisions of any nature contained within the Professional Services Agreement, by and between Consultant and MSI, dated April 1, 2014, as amended, (the "PSA"), are expressly understood and agreed to be material terms of this SOW as though fully set forth herein and hereby incorporated by reference. In the event of any conflict between the terms of this SOW set forth below and the PSA, the terms of the PSA control unless the specific provision of the PSA is identified as superseded. Any capitalized undefined terms herein will take the definitions assigned to them in the PSA.

Project Name: LTC Drop Ticket process

Start Date: October 13, 2017

Project/Services Oversight:

MSI: Jason Hartwig- Lead Client Manager
Consultant: Christy Pruett- VP of Application Fulfillment Services

1.0 Project/Services Description:

MSI will engage Consultant to provide daily calls to long-term care ("LTC") policy applicants to complete their LTC drop ticket process (each an "Application Specialist") per the terms of this SOW.

2.0 Term and Termination:

The term of this SOW shall begin on October 1, 2017 and shall continue for twelve (12) months; thereafter it shall continue on a month to month basis unless terminated: (i) by MSI as authorized by the PSA; or (ii) by Consultant upon ninety (90) days prior written notice to MSI. In any termination, MSI will pay for all Services actually rendered hereunder through the date of termination.

MSI can also require the removal any individual resource in accordance with 2.2(a)(i) of the PSA.

3.0 Resources/Services:

All Placed Personnel used to fulfill the obligations of this SOW will be employees of Consultant provided in accordance with 2.2(a)(i) of the PSA.

Services and Deliverables to be provided by Consultant via the Application Specialists:

- Consultant to Security Assertion Markup Language ("SAML") or Virtual Private Network ("VPN") into MSI's LTC portal;
- Each Application Specialist will have a user name and password;
- Each Application Specialist will complete the prequalified questions;
- Each Application Specialist will follow call campaign to complete the LTC application;
- Consultant will record all calls;
- Consultant will send calls to MSI upon request;
- Consultant will send monthly reporting to MSI LTC as set forth in Section 5.0 below;
- Consultant and MSI will work together to create scripting and all scripting will be approved in writing by MSI;
- Each Application Specialist will participate in training as discussed in Section 7.0 below; and
- Each Application Specialist will have the ability to work independently and in remote setting with virtual environment and team.

Required Qualifications of the Application Specialists:

- Ability to multi-task and prioritize.
- Excellent verbal and written communication skills with different levels with both internal and external audiences.
- Ability to meet high productivity demands.
- Strong decision making and problem solving skills.

Once a month, EMSI and MSI will determine if there is a need to adjust staffing to increase or decrease the number of calls. If additional staff is needed as a result of a volume change, EMSI will advise MSI in writing, which may be via e-mail to mkiigfer@transamerica.com and lillian.hodges@transamerica.com, of the change prior to the staff addition. In the event of a call volume change, EMSI agrees to provide MSI with a detailed breakdown of anticipated changes to monthly charges. EMSI will meet with MSI monthly to discuss stats and volumes and if there is a need to increase staff.

4.0 Service Levels:

Each new case assigned will be reviewed and called on within one (1) full business day of Consultant's receipt of a complete and accurate case. See Exhibit B for additional Service levels.

Consultant will randomly review and track the results of five percent (5%) of completed calls per month.

5.0 Reports/Deliverables:

Consultant will provide the following information to MSI in a single report (or multiple reports if requested by MSI) on a monthly basis:

1. Quality results by employee
2. Number of completed calls per day
3. Number of non-completed calls per day
4. Average handle time ("Average Handle Time") for completed interviews. Average handle time is defined as talk time plus after call work.
5. Average Handle Time for non-completed interviews
6. Average Handle Time for the prequalification calls
7. Avg. time to first client call to schedule appointment
8. Avg. time to connect with client and schedule appointment
9. % - Conversion Contact-to-Appointment
10. Avg. length of time to complete interview per individual life
11. % - appointments converted to mailed application
12. Avg. number of calls to schedule appointment
13. NET Conversion of drop tickets to mailed application

6.0 Location:

The Services set forth under this SOW will be performed at Consultant's location in Hewitt, TX. EMSI will have staff available during the following hours:

Monday-Friday 7:00 a.m. to 10:00 p.m. CT;

Saturday 9:00 a.m. to 1:00 p.m. CT (if calls are scheduled in advance); and

No scheduled calls Sunday.

7.0 Fees:

MSI will pay Consultant for the Services and Deliverables hereunder on an hourly basis as set forth in the table below. Consultant will submit the hours worked for each Application Specialist on a weekly basis and invoices to MSI on a monthly basis. In addition to the hourly rate below, MSI will pay \$2.65 per minute for any Application Specialist's use of the language line. Any script or form changes will be billed to MSI at \$125.00 per hour with prior written authorization. MSI also agrees to pay a one-time implementation fee of \$15,900.00 to cover all IT resources needed to initiate the Services (including without limitation, the establishment of desk access to computers, phone lines, monitors, a new 800 number, and email addresses), payable to EMSI up front; however this implementation fee is an estimate only and any requested changes to the scope of any work performed as a part of the implementation services, shall be added to the implementation at the \$125 hourly rate listed above. In the event the parties increased the number of Application Specialists hereunder, additional implementation fees will apply.

EMSI will immediately notify MSI in writing as soon as EMSI becomes aware that any of the estimated fees under this SOW may exceed any estimated amounts set forth herein. Under no circumstances may any fees under this SOW

exceed the estimated or specified amounts provided herein without the prior written consent of both Parties via an amendment or Change Order to this SOW.

It is estimated that each Application Specialist will work approximate forty (40) hours per week. While on the project MSI will be billed only for actual hours the Application Specialist is engaged in the Services specified in this SOW, or applicable training. MSI will not be billed for any time taken off for personal reasons, sick leave, vacation time, etc.

Role	Number of Resources	Hourly Rate (0- 40 Hours p/week)	Hourly Rate (Hours worked p/week greater than 45 hours)*	Hourly Rate While in Training	Packet Mailing
Application Specialist	4	\$28.00	\$42.00	\$28.00	\$12.00 per packet mailed for standard two (2) day shipping. Overnight shipping allowed with approval by MSI, and will be passed through at cost.

* MSI must give written approval prior to any Application Specialist billing greater than forty (40) hours in any one week.

* MSI must give approval prior to any additional Application Specialist being added.

• Training is expected to take place in Hewitt, TX in the first 2-3 weeks of a new Application Specialist being added to the engagement. MSI will provide the trainer(s) and training will be done one-on-one using remote desktop sharing.

Travel and expenses are not included in the estimated fees set forth above, and will be billed at cost to MSI. All travel expenses will comply with the PSA and the attached Exhibit A: Travel Expense Policy. Itemized expense reports will be provided with expense invoices and receipts. Consultant will make every effort to ensure travel expenses are reasonable or get approval prior to booking unusually expensive airfare/hotels (e.g. last minute airfare, airline rerouting, and hotel bookings during events).

8.0 Additional Provisions:

1. Record retention. Notwithstanding anything to the contrary in the PSA, EMSI will purge all recordings of calls with applicants after seven (7) years from the date of the call, unless otherwise required by applicable law.
2. EMSI may not subcontract out or assign any of the Services under this SOW without MSI's prior written consent, which MSI may grant, deny or withhold in its sole discretion.
3. Changes to this SOW may only be made via an amendment or Change Order to this SOW that is signed by both Parties.
4. MSI will provide each Application Specialist with a telephone and VPN access to the MSI network. Consultant will provide internet access reasonably believed to be reliable and their own working space that is reasonably secure and free from distractions.

IN WITNESS WHEREOF, the parties have entered into this SOW as of the Effective Date.

Examination Management Services, Inc.

By: *Christy Pruitt* 10/12/17
 Signature of Authorized Officer Date

Money Services, Inc.

By: *B.* 10/12/2017
 Signature of Authorized Officer

Christy Pruitt Vice President

Tjeerd Edelman

Vice President

Print Name and Title

Print Name and Title

Exhibit A

Travel Expense Policy

Receipts required for reimbursement of all expenses, except for POV Mileage.

Air Travel

Airfare: Standard coach fares, best available at time of booking. Please make travel as far in advance as possible (14+ days, ideally).

Baggage: Actual expenses with receipts. Not to exceed two checked bags.

Airport Parking: Actual expenses with receipts. Long-term or off airport parking only.

Ground Transportation

Taxi: Cab fare and reasonable tips (<20%) reimbursed.

Rental Car: Compact or Intermediate (best available rates). No rental car insurance should be purchased.

Gasoline – Rental Car: Actual expenses with receipts. No pre-pay. Rental car should be filled up prior to returning.

Privately Owned Vehicle (POV): Reimbursed at published IRS Standard Mileage Rates for Business Miles (currently 54 cents/mile). See IRS website for current rates. *Gas / Maintenance costs not covered.*

Miscellaneous Parking, Tolls, Ferries – Actual expenses with receipts.

Lodging

Hotel Rooms: Reasonable standard accommodations. Prices vary based on season, special events, etc. Prior management approval required for hotel rooms that cost more than \$150 per night (before taxes).

Miscellaneous: No reimbursement for in-room entertainment, valet services, or laundry services.

Telephone & Internet: Not covered.

Meals

Limited to actual expenses, including tips, with receipts. Not to exceed \$50 per day. Receipts in excess of stated maximums will only be reimbursed up to that maximum.

Miscellaneous

Entertainment Expenses: Not covered.

Shipping & Postage: Actual expenses with receipts.

Exhibit B

Performance Metrics

1. **Service Level Agreement.** EMSI shall perform the Services at all times during the Term of this SOW in accordance with specific performance standards set forth herein ("Service Level Agreement" or "SLA"). The SLA below indicates the levels of performance EMSI must achieve for each service metric ("Service Level").

1.1 **SLAs for the SOW.**

<u>Service Levels:</u>	<u>Service Level Credits:</u> (based on the specified percentage of Service fees payable under this SOW for the month in which the Performance Failure occurs. For clarity, in no event shall Service Level credits apply to any implementation fees, hourly IT charges or expenses from third parties passed through under the SOW (i.e. language line fees; mailing fees).)
Excel spreadsheet will be sent daily to MSI with updates on the pending cases.	1% of monthly Service fees in impacted month.
85% of the time, EMSI shall make contact with LTC policy applicant no earlier than two (2) business hours after receipt of a complete and accurate ticket, but no later than one (1) full business day after receipt of a complete and accurate ticket. This Service Level excludes cases put on hold or cancelled by MSI, as well as failures or delays attributable to MSI or the applicant.	1% of impacted Services in any given month where EMSI fails to meet the Service Level
85% of the time, EMSI shall contact LTC policy applicant every business day, two (2) times per business day, 1 voicemail per day for 5 business days. Day 6 if no response from the LTC policy applicant, contact MSI for further handling. This Service Level excludes cases put on hold or cancelled by MSI, as well as failures or delays attributable to MSI or the applicant.	1% of impacted Services in any given month where EMSI fails to meet the Service Level

2. **Service Level Measurement.** EMSI shall implement and operate all measurement and monitoring tools and procedures required to measure and report its performance relative to the applicable SLA. Each SLA will be measured on at least a monthly basis. EMSI shall provide, as part of EMSI's monthly performance reports, a set of reports – in a format to be determined by MSI – to verify EMSI's performance and compliance with the Service Level Agreement ("Performance Reports"). The SLA measurement, monitoring, and reporting processes will be subject to audit by MSI in accordance with the PSA.

3. **Service Level Credits.**

(a) **Calculation of Service Level Credits.** EMSI's failure to meet the Service Level for any Service Level (each a "Performance Failure") shall permit MSI to deduct the applicable credit against the applicable Fee payable for that Service, as calculated in accordance with this Exhibit and SOW ("Service Level Credits"). For clarity, in no event shall Service Level credits apply to any implementation fees, hourly IT charges or expenses from third parties passed through under the SOW (i.e. language line fees; mailing fees). Service Level Credits will be calculated each month for each Performance Failure.

(b) **Issuance of Credits.** EMSI will reduce the amount payable by MSI on the next Invoice by the amount of Service Level Credits MSI received during the applicable month. In no event shall Service Level credits exceed 3% of a monthly Invoice, and monthly Service Level Fees will be capped at 3% per month.

5. **Root Cause Analysis.** EMSI will be required to conduct, at its expense, a root cause analysis for each failure to meet any Service Level for any consecutive three (3) month period. Upon determination of the cause of such

failure, EMSI will provide to MSI an additional report that details the results of the root cause analysis, and which details any measures that should be taken to minimize the possibility that such failures will re-occur. To the extent that the root cause analysis indicates that EMSI's failure to meet the Service Level was caused by EMSI, EMSI will use commercially reasonable means to correct the problem at no additional cost to MSI.

AMENDMENT TO PROFESSIONAL SERVICES AGREEMENT

This Amendment (this "Amendment") is to the PROFESSIONAL SERVICES AGREEMENT, dated April 1, 2014 (the "Agreement") by and between Money Services, Inc. ("MSI") and Examination Management Services, Inc. ("Service Provider"). This Amendment shall become effective as of January 1, 2018 ("Effective Date").

WHEREAS, the parties desire to memorialize certain events to amend the Agreement as set forth more fully below.

NOW, THEREFORE, in consideration of the mutual promises and covenants contained herein, the parties agree as follow:

1. Exhibit C to the Agreement is hereby amended by adding the below requirements under Telephone Interviews ("Interview(s)":
 - During normal business hours, point of sale ("POS") calls will average 30 seconds or less average speed of answer, 5% or less of the calls go to voicemail, 5% or less of the call are abandoned, meaning 95% of incoming calls during business hours will be answered.
 - Three months from the Effective Date of this Amendment, the parties agree to review the POS interview statistics above to see volume, call length, and service levels. Six months from the Effective Date of this Amendment the parties agree to review pricing for the Medsup POS interview only. At that time, the price may be renegotiated and/or Service Level Agreements may be changed upon mutual agreement.
2. Exhibit D to the Agreement is hereby amended by deleting it in its entirety and replacing it with the attached new Exhibit D.
3. Except as specifically amended herein, the Agreement shall remain in full force and effect in accordance with its terms. Capitalized terms not specifically defined herein shall have the same meaning ascribed to them under the Agreement. This Amendment may be executed in one or more counterparts, each of which shall be an original and all of which taken together shall constitute one and the same instrument.

IN WITNESS WHEREOF, the parties hereto have executed this Amendment as of the date set forth above.

Money Services, Inc.

By: Kevin M. Crist
(Authorized Signature)

Kevin Crist
(Name)

Vice President
(Title)
2/27/2018
(Execution Date)

Examination Management Services, Inc.

By: Chad M. Gross
(Authorized Signature)

Chad M. Gross
(Name)

Chief Operating Officer
(Title)
03-23-2018
(Execution Date)

EXHIBIT D
Underwriting Services and Fees

Medical Records		
Description	Home Office Orders Pricing	Brokerage Orders Pricing
All Case Fee (includes facility fee up to \$100)	\$56.00	\$60.00
Case Closed w/o Records service fee	\$15.00	-
OPTIONAL SERVICES		
Rush Handling	\$10.00	\$10.00
Special Authorization Fee - to upload to the website	\$4.00	\$4.00
Special Authorization Fee - to obtain the special authorization from applicant	\$12.00	\$12.00

Paramedical Services		
*Kits – any kit fee increase by a laboratory during the term of this Agreement will be passed forward as an increase to MSI at cost plus twenty percent (20%)		
Billing Code	Description	Pricing
1	Physician Part 2 Exam	\$90.10
2	Exam Part 2 (standalone)	\$45.01
4	EKG (standalone)	\$57.05
5	Vitals (standalone) Recheck	\$73.39
14	Physician EKG	\$34.04
15	Urine Collection (standalone)	\$38.04
19	Cancel / Refusal / No Show at the Door	\$26.50
		\$1.80 per minute + pass through from supplier
30	Miscellaneous - Language Line	\$464.46
31	Physician Treadmill	Sec below
110	Gasoline Surcharge	\$2.00
116	Case Management Service / Imaging	\$66.50
207	Exam Part 2 + EKG	\$76.73
366	Vitals – Blood + Urine + EKG	\$38.04
409	Saliva (standalone)	\$11.00
490	App Packet Part I Handling (add on)	\$45.00
491	App Packet Part I Handling (standalone)	\$74.99
749	Vitals – Urine	\$11.70
800	Saliva Kit* – CRL	\$11.81
801	Blood Kit* – CRL	\$14.89
804	Blood Kit* – LabOne	\$17.66
820	Urine Kit* – CRL	\$17.40
823	Urine Kit* – LabOne	\$45.04
830	Saliva Kit* – LabOne	\$60.00
850	DBS Kit* – CRL	\$15.22
857	DBS Kit* – LabOne	\$15.22
18 & 1018	Blood + Urine or Blood only	\$17.40
1120	Vitals – Blood + Urine	\$17.40
1126	Exam Part 2 + Blood + Urine	\$73.55

1160	Exam Part 2 + Blood + Urine + EKG	\$112.43
6000	IGO Mobile Examiner	\$13.50
6006	IGO Mobile Max	\$12.00
TBD	Telexam ID Check	\$50.00
TBD	One Touch	\$3.00
Fuel Surcharge		
	When the price of gas exceeds \$2.75 per gallon, MSI will pay a fuel surcharge. 100% of this fuel surcharge is allocated back to the examiner to defray their fuel cost. Surcharge is applied to cases the month following the fuel cost assessment.	Average Price per Gallon
		\$2.74 or Less
		\$2.75 - \$3.24
		\$3.25 - \$3.74
		\$3.75 - \$4.24
		Above \$4.25
Geographical Surcharge		Surcharge
	Geographical Surcharge - up charge to rate listed above	California, DC, NY, Boston, Chicago
		1.25 times the Service Fees
	Geographical Surcharge - up charge to rate listed above	Puerto Rico, Guam, Alaska, Hawaii
		2 times the Service Fees

Paramedical Service Notes:

1. Service Provider may accept order for initial underwriting requirements based on the product grids.
2. Combination rates are to be billed to MSI when applicable.
3. Service Provider needs to ask if an application has been signed by the applicant, what state it was signed in by the applicant, and have that information available to MSI.
4. Requests outside of initial underwriting requirements require Service Provider home office approval.
5. A twenty (20%) percent discount of the impacted service fee shall occur by Service Provider when an exam is unusable by MSI when received. In no event shall such discount apply to any pass through charges such as kit fees, fuel or postage.

Inspection Reports				
High Rate and Data Searches	Report Name	Report Number	Pricing	
1201	SPOUSAL INTERVIEW	F007	\$8.92	
1204	AMPLIFIED NO SOURCES INTERVIEW	F011	\$42.03	
1206	BUSINESS AMP W/SOURCES 9/14	FR16	\$55.69	
1231	BUSINESS BENEFICIARY REPORT INTERVIEW	Q022	\$36.53	
1253	CRIMINAL HISTORY INTERVIEW	Q060	\$8.41	
1200	QUICK E-SEARCH - DATA SEARCH	F001	\$12.84	
1230	BANKRUPTCY INFORMATION - DATA SEARCH	Q032	\$10.80	
1234	CREDIT SUMMARY - DATA SEARCH	Q025	\$10.80	
1254	CRIMINAL RECORDS - DATA SEARCH	Q074	\$24.46	
	CRIMINAL RECORDS - DETAIL SEARCH			

Interviews				
Billing Code	Report Name	Report Number	Standalone	With other Interview Services
1200	PHI FE 4/15	F001	\$23.49	
1201	PHI SR 4/15	F002	\$31.95	
1202	TRANSAM HEALTH INTERVIEW 3/15	F003	\$27.00	
1203	PHI-SI	F004	\$13.04	
1200	MEDSUP INTERVIEW	F005	\$25.00	
	MEDSUP INTERVIEW – POINT OF SALE		\$28.75	
1205	JUVENILE REPORT	F006	\$19.00	
1206	PHI-DI 7/14	F007	\$26.44	
1204	FE REINSTATE 5/15	F008 or F009	\$23.49	
1207	SR REINSTATE 5/15	F010	\$31.95	
1209 &				
1220	AGENT QUALITY INTERVIEW	Q001&Q101	\$8.41	\$2.90
1211 &				
1222	AD HOC QUESTIONNAIRE	Q003 & Q103	\$8.25	\$4.68
1213 &				
1224	ANEMIA QUESTIONNAIRE	Q005 & Q105	\$8.66	\$6.57
1214 &				
1225	ARTHRITIS QUESTIONNAIRE	Q006 & Q106	\$9.17	\$7.34
1215 &				
1226	BACK/NECK PAIN QUESTIONNAIRE	Q007 & Q107	\$10.80	\$8.41
1216 &				
1227	CANCER QUESTIONNAIRE	Q008 & Q108	\$8.66	\$6.57
1218 &				
1229	DIABETES QUESTIONNAIRE	Q010 & Q110	\$10.80	\$8.41
1219 &				
1230	DEPRESSION/MENTAL/NERVOUS QN	Q011 & Q111	\$11.31	\$8.92
1210 &				
1221	DISABILITY QUESTIONNAIRE 3/15	Q002 & Q102	\$8.41	\$5.55
1212 &				
1223	GEN. MEDICAL FOLLOW-UP	Q004 & Q104	\$3.41	\$3.41
1217 &				
1228	CEREBRAL PALSY QUESTIONNAIRE	Q009 & Q109	\$8.41	\$3.41
1230 &				
1258	CHRONIC PAIN	Q046 & Q146	\$12.58	\$11.06
1230 &				
1271	CRIMINAL HISTORY INTERVIEW	Q060	\$8.41	\$8.41
1230 &				
1297	CRIMINAL HISTORY QUESTIONNAIRE	Q160	\$8.41	\$8.41
1231 &				
1293	GASTROINTESTINAL QUESTIONNAIRE	Q012 & Q112	\$9.17	\$7.34
1232 &				
1260	HEART DISEASE/DISORDER QN'S	Q013 & Q113	\$9.99	\$7.90
1233 &				
1261	HEART MURMUR QUESTIONNAIRE	Q014 & Q114	\$8.41	\$6.01
1234 &				
1262	HEPATITIS QUESTIONNAIRE	Q015 & Q115	\$12.08	\$9.48

1235 & 1263	Hysterectomy Questionnaire	Q016 & Q116	\$8.41	\$4.48
1236 & 1264	High Blood Pressure Questions	Q017 & Q117	\$8.66	\$6.57
1237 & 1265	Lupus Questionnaire	Q018 & Q118	\$8.41	\$6.01
1238 & 1266	Multiple Sclerosis Questions	Q019 & Q119	\$9.17	\$7.34
1239 & 1267	Pregnancy Questionnaire	Q020 & Q120	\$8.41	\$4.48
1240 & 1268	Respiratory Disorder QN's	Q021 & Q121	\$8.66	\$6.57
1241 & 1269	Seizure Questionnaire	Q022 & Q122	\$11.31	\$8.92
1242 & 1272	Skin Cancer Questionnaire	Q023 & Q123	\$8.41	\$6.01
1243 & 1273	Sleep Apnea Questionnaire	Q024 & Q124	\$9.17	\$7.34
1244 & 1274	Stroke Questionnaire	Q025 & Q125	\$9.99	\$7.90
1245 & 1275	Thyroid Questionnaire	Q026 & Q126	\$8.41	\$5.55
1246 & 1276	Ulcer Questionnaire	Q027 & Q127	\$8.41	\$5.55
1247 & 1277	Occupation & Income QN's	Q028 & Q128	\$8.41	\$4.99
1248 & 1278	Foreign Travel	Q029 & Q129	\$8.41	\$1.83
1249 & 1279	Military Questionnaire	Q030 & Q130	\$11.31	\$8.92
1250 & 1280	Tobacco Questionnaire	Q031 & Q131	\$8.41	\$1.12
1251 & 1281	Alcohol/Drug Questionnaire	Q032 & Q132	\$8.41	\$6.01
1252 & 1282	Driving Questionnaire	Q033 & Q133	\$8.41	\$4.48
1253 & 1283	Aviation Questionnaire	Q034 & Q134	\$14.98	\$11.57
1254 & 1284	Avocation Questionnaire	Q035 & Q135	\$12.08	\$9.48
1257 & 1287	FL Avocation Questionnaire	Q038 & Q138	\$11.31	\$8.92
1259 & 1288	Residency Questionnaire	Q040 & Q140	\$8.41	\$4.99
1255	NY Avocation Questionnaire	Q036	\$12.08	\$9.48
1256	MD Avocation Questionnaire	Q037	\$11.31	\$8.92
1294 & 1295	Migraine Headache Questions Unemployed Due to DI Questionnaire	Q045 & Q145 QN42 & QN142	\$10.50 \$2.26	\$7.90 \$2.26
	Criminal Records	QN43 & QN143	\$25.20	\$19.66

	BANKRUPTCY INFORMATION	QN44 & QN144 QN47 & QN147 QN48& QN148	\$11.13	\$8.68
	HABITS QUESTIONNAIRE		\$13.81	\$10.77
	MEDICATIONS QUESTIONNAIRE		\$14.70	\$11.47

1. All pricing shall remain in effect from January 1, 2018 – April 30, 2019. After April 30, 2019, Service Provider shall have the right to increase pricing annually in an amount that equal to the change in the U.S. Bureau of Labor Statistics Consumer Price Index for the most recently completed calendar year or three percent (3%), whichever is less.
2. Fees billed outside the above guidelines may be subject to non-payment.



Certificate Of Completion

Envelope Id: 90B918389D1B4BC0B1BA1468E846779F

Subject: Please DocuSign: 20180101_EMSI_Amedment.pdf

Source Envelope:

Document Pages: 6

Signatures: 1

Certificate Pages: 1

Initials: 0

AutoNav: Enabled

EnvelopeId Stamping: Enabled

Time Zone: (UTC-08:00) Pacific Time (US & Canada)

Status: Completed

Envelope Originator:

Melissa Pump

4333 Edgewood Rd NE

Cedar Rapids, IA 52499

melissa.pump@transamerica.com

IP Address: 162.123.17.80

Record Tracking

Status: Original

2/23/2018 9:18:32 AM

Holder: Melissa Pump

melissa.pump@transamerica.com

Location: DocuSign

Signer Events

Kevin Crist

Kevin.Crist@transamerica.com

Vice President

Money Services, Inc.

Security Level: Email, Account Authentication
(None)

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

Signature

Timestamp

Sent: 2/23/2018 9:20:05 AM

Viewed: 2/27/2018 2:55:50 AM

Signed: 2/27/2018 2:56:01 AM

In Person Signer Events

Signature

Timestamp

Editor Delivery Events

Status

Timestamp

Agent Delivery Events

Status

Timestamp

Intermediary Delivery Events

Status

Timestamp

Certified Delivery Events

Status

Timestamp

Carbon Copy Events

Status

Timestamp

Notary Events

Signature

Timestamp

Envelope Summary Events

Status

Timestamps

Envelope Sent

Hashed/Encrypted

2/23/2018 9:20:06 AM

Certified Delivered

Security Checked

2/27/2018 2:55:50 AM

Signing Complete

Security Checked

2/27/2018 2:56:01 AM

Completed

Security Checked

2/27/2018 2:56:01 AM

Payment Events

Status

Timestamps

**AMENDMENT NO. 2 TO
PROFESSIONAL SERVICES AGREEMENT**

This Amendment No. 2 (this "Amendment") is to the PROFESSIONAL SERVICES AGREEMENT, dated April 1, 2014 (the "Agreement") by and between Money Services, Inc. ("MSI") and Examination Management Services, Inc. ("Service Provider"). This Amendment shall become effective as of January 1, 2019 ("Effective Date").

WHEREAS, the parties previously entered into the Agreement, and Amendment ("Amendment No. 1") dated January 1, 2018; and

WHEREAS, the parties desire to memorialize certain events to amend the Agreement and Amendment No. 1 as set forth more fully below.

NOW, THEREFORE, in consideration of the mutual promises and covenants contained herein, the parties agree as follow:

1. Exhibit D to the Agreement and Amendment No. 1 is hereby amended so that the "Geographical Surcharge" section of the Paramedical Services table is deleted and replaced with the following:

Geographical Surcharge		
Geographical Surcharge - up charge to rate listed above	DC, Boston, Chicago	1.25 times the Service Fees
Geographical Surcharge - up charge to rate listed above	California, New York	1.50 times the Service Fees
Geographical Surcharge - up charge to rate listed above	Puerto Rico, Guam, Alaska, Hawaii	2 times the Service Fees

2. Except as specifically amended herein, the Agreement shall remain in full force and effect in accordance with its terms. Capitalized terms not specifically defined herein shall have the same meaning ascribed to them under the Agreement. This Amendment may be executed in one or more counterparts, each of which shall be an original and all of which taken together shall constitute one and the same instrument.

IN WITNESS WHEREOF, the parties hereto have executed this Amendment as of the date set forth above.

Money Services, Inc.

By:

Catherine Luoma
(Authorized Signature)

Catherine Luoma

(Name)

Vice President

(Title)

1/7/2019

(Execution Date)

Examination Management Services, Inc.

By:

Greg C. James
(Authorized Signature)

Greg C. James
(Name)

Chief Operating Officer
(Title)

12/31/2018

(Execution Date)



Certificate Of Completion

Envelope Id: D63E79FB80494EE9B9CC0451CC0F2E3E
 Subject: CW2314223 - Money Services Amendment No 2 to PSA 12-31-18 (002).pdf
 Source Envelope:
 Document Pages: 1 Signatures: 1
 Certificate Pages: 5 Initials: 1
 AutoNav: Enabled
 Envelope Stamping: Enabled
 Time Zone: (UTC-08:00) Pacific Time (US & Canada)

Status: Completed
 Envelope Originator:
 Melissa Pump
 6400 C St. SW
 Cedar Rapids, IA 52499
 melissa.pump@transamerica.com
 IP Address: 216.109.110.11

Record Tracking

Status: Original 1/7/2019 5:58:26 AM	Holder: Melissa Pump melissa.pump@transamerica.com	Location: DocuSign
-----------------------------------------	-------------------------------------------------------	--------------------

Signer Events

Signer	Signature	Timestamp
Linda McFadden Linda.McFadden@transamerica.com Lead Vendor Manager Underwriting - Vendor Management Security Level: Email, Account Authentication (None)		Sent: 1/7/2019 5:59:44 AM Viewed: 1/7/2019 6:01:35 AM Signed: 1/7/2019 6:01:48 AM
	Signature Adoption: Pre-selected Style Using IP Address: 162.123.17.80	

Electronic Record and Signature Disclosure:

Accepted: 10/2/2018 8:10:53 AM
 ID: 680b8712-737d-43a7-8486-958a8b90c423

Catherine Luoma
catherine.luoma@transamerica.com
Vice President
Transamerica Procurement
Security Level: Email, Account Authentication
(None)

Sent: 1/7/2019 6:01:49 AM
 Viewed: 1/7/2019 9:59:58 AM
 Signed: 1/7/2019 10:00:03 AM

Electronic Record and Signature Disclosure:

Not Offered via DocuSign

In Person Signer Events

Signer	Timestamp
--------	-----------

Editor Delivery Events

Status	Timestamp
--------	-----------

Agent Delivery Events

Status	Timestamp
--------	-----------

Intermediary Delivery Events

Status	Timestamp
--------	-----------

Certified Delivery Events

Status	Timestamp
--------	-----------

Carbon Copy Events

Status	Timestamp
--------	-----------

Notary Events

Signer	Timestamp
--------	-----------

Envelope Summary Events

Status	Timestamps
--------	------------

Envelope Sent
 Certified Delivered
 Signing Complete
 Completed

Hashed/Encrypted	1/7/2019 6:01:49 AM
Security Checked	1/7/2019 9:59:58 AM
Security Checked	1/7/2019 10:00:03 AM
Security Checked	1/7/2019 10:00:03 AM

Payment Events	Status	Timestamps
Electronic Record and Signature Disclosure		

ELECTRONIC RECORD AND SIGNATURE DISCLOSURE

From time to time, Transamerica Procurement (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through your DocuSign, Inc. (DocuSign) Express user account. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to these terms and conditions, please confirm your agreement by clicking the 'I agree' button at the bottom of this document.

Getting paper copies

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. For such copies, as long as you are an authorized user of the DocuSign system you will have the ability to download and print any documents we send to you through your DocuSign user account for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a \$0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

Withdrawing your consent

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

Consequences of changing your mind

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. To indicate to us that you are changing your mind, you must withdraw your consent using the DocuSign 'Withdraw Consent' form on the signing page of your DocuSign account. This will indicate to us that you have withdrawn your consent to receive required notices and disclosures electronically from us and you will no longer be able to use your DocuSign Express user account to receive required notices and consents electronically from us or to sign electronically documents from us.

All notices and disclosures will be sent to you electronically

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through your DocuSign user account all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

How to contact Transamerica Procurement:

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:

To contact us by email send messages to: procurement@transamerica.com

To advise Transamerica Procurement of your new e-mail address

To let us know of a change in your e-mail address where we should send notices and disclosures electronically to you, you must send an email message to us at procurement@transamerica.com and in the body of such request you must state: your previous e-mail address, your new e-mail address. We do not require any other information from you to change your email address..

In addition, you must notify DocuSign, Inc to arrange for your new email address to be reflected in your DocuSign account by following the process for changing e-mail in DocuSign.

To request paper copies from Transamerica Procurement

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an e-mail to procurement@transamerica.com and in the body of such request you must state your e-mail address, full name, US Postal address, and telephone number. We will bill you for any fees at that time, if any.

To withdraw your consent with Transamerica Procurement

To inform us that you no longer want to receive future notices and disclosures in electronic format you may:

- i. decline to sign a document from within your DocuSign account, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;
- ii. send us an e-mail to procurement@transamerica.com and in the body of such request you must state your e-mail, full name, IS Postal Address, telephone number, and account number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

Required hardware and software

Operating Systems:	Windows2000? or WindowsXP?
Browsers (for SENDERs):	Internet Explorer 6.0? or above
Browsers (for SIGNERS):	Internet Explorer 6.0?, Mozilla FireFox 1.0, NetScape 7.2 (or above)
Email:	Access to a valid email account
Screen Resolution:	800 x 600 minimum
Enabled Security Settings:	<ul style="list-style-type: none">• Allow per session cookies

	<ul style="list-style-type: none">• Users accessing the internet behind a Proxy Server must enable HTTP 1.1 settings via proxy connection
--	---------------------------------------------------------------------------------------------------------------------------------------------------------

** These minimum requirements are subject to change. If these requirements change, we will provide you with an email message at the email address we have on file for you at that time providing you with the revised hardware and software requirements, at which time you will have the right to withdraw your consent.

Acknowledging your access and consent to receive materials electronically

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please verify that you were able to read this electronic disclosure and that you also were able to print on paper or electronically save this page for your future reference and access or that you were able to e-mail this disclosure and consent to an address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format on the terms and conditions described above, please let us know by clicking the 'I agree' button below.

By checking the 'I Agree' box, I confirm that:

- I can access and read this Electronic CONSENT TO ELECTRONIC RECEIPT OF ELECTRONIC RECORD AND SIGNATURE DISCLOSURES document; and
- I can print on paper the disclosure or save or send the disclosure to a place where I can print it, for future reference and access; and
- Until or unless I notify Transamerica Procurement as described above, I consent to receive from exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to me by Transamerica Procurement during the course of my relationship with you.

Change Order No. 1 to Statement of Work LTC Drop Ticket process

This Change Order ("Change Order") is dated as of February 16, 2018 ("Execution Date"), and is by and between Money Services, Inc. ("MSI") and Examination Management Services, Inc. ("Consultant"). This Change Order is incorporated into that certain Statement of Work LTC Drop Ticket process dated October 12, 2017 ("SOW") to the Professional Services Agreement dated April 1, 2014 ("Agreement"), between Consultant and MSI. The terms and conditions that are specific to this Change Order are set forth below. In the event of a conflict between the provisions of this Change Order and any prior change order, the provisions of this Change Order shall control such conflict. In the event of a conflict between the provisions of this Change Order and the SOW, the provisions of this Change Order will control such conflict. In the event of a conflict between the provisions of this Change Order and the Agreement, the provisions of the Agreement will control unless the specific provision of the Agreement is identified as superseded.

1.0 Change Summary:

Updating the pricing structure to add pricing for instances where states require a licensed representative complete the application.

2.0 Sections of the SOW modified by this Change Order:

2.1 The following is added to Section 7 of the SOW:

Notwithstanding anything to the contrary, if applicable law, rule or regulation requires a licensed agent to complete all or a portion(s) of the application, Consultant shall ensure that a licensed agent shall be utilized for the same and MSI shall pay an additional \$17.00 fee in addition to any other applicable charges in the SOW for each such occurrence.

THE PARTIES ACKNOWLEDGE THAT THEY HAVE READ THIS CHANGE ORDER, UNDERSTAND IT, AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS. FURTHER, THE PARTIES AGREE THAT THE COMPLETE AND EXCLUSIVE STATEMENT OF THE AGREEMENT BETWEEN THE PARTIES RELATING TO THIS SUBJECT SHALL CONSIST OF 1) THIS CHANGE ORDER, 2) PRIOR CHANGE ORDERS, IF ANY, 3) THE SOW, AND 4) THE AGREEMENT (INCLUDING THE EXHIBITS THERETO), INCLUDING THOSE CHANGE ORDERS MADE EFFECTIVE BY THE PARTIES IN THE FUTURE. THIS STATEMENT OF THE CHANGE ORDER BETWEEN THE PARTIES SUPERSEDES ALL PROPOSALS OR OTHER PRIOR AGREEMENTS, ORAL OR WRITTEN, AND ALL OTHER COMMUNICATIONS BETWEEN THE PARTIES RELATING TO THE SUBJECT DESCRIBED HEREIN.

IN WITNESS WHEREOF, the parties have entered into this SOW as of the Effective Date.

MONEY SERVICES, INC.

By: Kevin M. Crist
Name: Kevin Crist
Title: Vice President
Date: 2/21/2018

EXAMINATION MANAGEMENT SERVICES,
INC.

By: Christy Pruitt
Name: Christy Pruitt
Title: Vice President, Operations
Date: 2/20/18



Certificate Of Completion

Envelope Id: 6E67C6EF280B4CCF8E4405A496937BE7
 Subject: Please DocuSign: 20180216_Money Services Change Order No 1 to SOW LTC final signed.pdf
 Source Envelope:
 Document Pages: 1 Signatures: 1
 Certificate Pages: 1 Initials: 0
 AutoNav: Enabled
 Envelope Stamping: Enabled
 Time Zone: (UTC-06:00) Central Time (US & Canada)

Envelope Originator:
 Transamerica Procurement
 4333 Edgewood Rd NE
 Cedar Rapids, IA 52499
 procurement@transamerica.com
 IP Address: 162.123.17.82

Record Tracking

Status: Original 2/21/2018 8:53:38 AM	Holder: Transamerica Procurement procurement@transamerica.com	Location: DocuSign
------------------------------------------	------------------------------------------------------------------	--------------------

Signer Events

Kevin Crist
 Kevin.Crist@transamerica.com
 Vice President
 Money Services, Inc.
 Security Level: Email, Account Authentication
 (None)

Signature

Timestamp

Sent: 2/21/2018 8:55:04 AM
 Viewed: 2/21/2018 9:56:19 AM
 Signed: 2/21/2018 9:56:53 AM

Electronic Record and Signature Disclosure:
 Not Offered via DocuSign

In Person Signer Events

Signature

Timestamp

Editor Delivery Events

Status

Timestamp

Agent Delivery Events

Status

Timestamp

Intermediary Delivery Events

Status

Timestamp

Certified Delivery Events

Status

Timestamp

Carbon Copy Events

Status

Timestamp

Matthew Sieck
 matthew.sieck@transamerica.com

Sent: 2/21/2018 9:56:54 AM
 Viewed: 2/21/2018 10:13:49 AM

Electronic Record and Signature Disclosure:
 Not Offered via DocuSign

Notary Events

Signature

Timestamp

Envelope Summary Events

Status

Timestamps

Envelope Sent
 Certified Delivered
 Signing Complete
 Completed

Hashed/Encrypted
 Security Checked
 Security Checked
 Security Checked

2/21/2018 9:56:54 AM
 2/21/2018 9:56:54 AM
 2/21/2018 9:56:54 AM
 2/21/2018 9:56:54 AM

Payment Events

Status

Timestamps

Change Order No. 2 to Statement of Work LTC Drop Ticket process

This Change Order ("Change Order") is dated as of October 26, 2018 ("Execution Date"), and is by and between Money Services, Inc. ("MSI") and Examination Management Services, Inc. ("Consultant"). This Change Order is incorporated into that certain Statement of Work LTC Drop Ticket process dated October 12, 2017 and Change Order No. 1 dated February 16, 2018 (as amended, "SOW") to the Professional Services Agreement dated April 1, 2014 ("Agreement"), between Consultant and MSI. The terms and conditions that are specific to this Change Order are set forth below. In the event of a conflict between the provisions of this Change Order and any prior change order, the provisions of this Change Order shall control such conflict. In the event of a conflict between the provisions of this Change Order and the SOW, the provisions of this Change Order will control such conflict. In the event of a conflict between the provisions of this Change Order and the Agreement, the provisions of the Agreement will control unless the specific provision of the Agreement is identified as superseded.

1.0 Change Summary:

Updating the permitted service locations used by Consultant.

2.0 Sections of the SOW modified by this Change Order:

2.1 The first sentence of Section 6.0 is amended to read as follows:

The Services set forth under this SOW will be performed at Consultant's location in either Waco, Texas or Hewitt, Texas.

THE PARTIES ACKNOWLEDGE THAT THEY HAVE READ THIS CHANGE ORDER, UNDERSTAND IT, AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS. FURTHER, THE PARTIES AGREE THAT THE COMPLETE AND EXCLUSIVE STATEMENT OF THE AGREEMENT BETWEEN THE PARTIES RELATING TO THIS SUBJECT SHALL CONSIST OF 1) THIS CHANGE ORDER, 2) PRIOR CHANGE ORDERS, IF ANY, 3) THE SOW, AND 4) THE AGREEMENT (INCLUDING THE EXHIBITS THERETO), INCLUDING THOSE CHANGE ORDERS MADE EFFECTIVE BY THE PARTIES IN THE FUTURE. THIS STATEMENT OF THE CHANGE ORDER BETWEEN THE PARTIES SUPERSEDES ALL PROPOSALS OR OTHER PRIOR AGREEMENTS, ORAL OR WRITTEN, AND ALL OTHER COMMUNICATIONS BETWEEN THE PARTIES RELATING TO THE SUBJECT DESCRIBED HEREIN.

IN WITNESS WHEREOF, the parties have entered into this SOW as of the Effective Date.

MONEY SERVICES, INC.

By: Catherine Luoma

RM

Name: Catherine Luoma

Title: Vice President

Date: 11/30/2018

EXAMINATION MANAGEMENT SERVICES, INC.

By: Christy Pruett

Name: Christy Pruett

Title: AVP, New Business

Date: 11/30/2018



Certificate Of Completion

Envelope Id: 6D6B4817561F4D17BB16A03E480A5425
 Subject: CW2312928 - 20181130_EMSI_ChangeOrderNo2to SOWLTC.pdf
 Source Envelope:
 Document Pages: 1
 Certificate Pages: 5
 AutoNav: Enabled
 Enveloped Stamping: Enabled
 Time Zone: (UTC-08:00) Pacific Time (US & Canada)

Status: Completed

Envelope Originator:
 Melissa Pump
 6400 C St. SW
 Cedar Rapids, IA 52499
 melissa.pump@transamerica.com
 IP Address: 216.109.110.11

Record Tracking

Status: Original	Holder: Melissa Pump	Location: DocuSign
11/30/2018 10:02:31 AM	melissa.pump@transamerica.com	

Signer Events

Christy Pruitt
 cpruett@emsinet.com
 AVP, New Business
 Security Level: Email, Account Authentication
 (None)

Signature

Signature Adoption: Pre-selected Style
 Using IP Address: 64.124.107.50

Timestamp

Sent: 11/30/2018 10:04:50 AM
 Viewed: 11/30/2018 10:16:09 AM
 Signed: 11/30/2018 10:16:37 AM

Electronic Record and Signature Disclosure:

Accepted: 11/30/2018 10:16:09 AM
 ID: 23dd8b6c-9889-4d50-96ae-9562158a35fb

Linda McFadden
 Linda.McFadden@transamerica.com
 Lead Vendor Manager
 Underwriting - Vendor Management
 Security Level: Email, Account Authentication
 (None)

Signature Adoption: Pre-selected Style
 Using IP Address: 162.123.17.80

Sent: 11/30/2018 10:16:38 AM
 Viewed: 11/30/2018 10:23:08 AM
 Signed: 11/30/2018 10:23:17 AM

Electronic Record and Signature Disclosure:

Accepted: 10/2/2018 8:10:53 AM
 ID: 680b8712-737d-43a7-8486-958a8b90c423

Catherine Luoma
 catherine.luoma@transamerica.com
 Vice President
 Transamerica Procurement
 Security Level: Email, Account Authentication
 (None)

Signature Adoption: Pre-selected Style
 Using IP Address: 198.39.4.70

Sent: 11/30/2018 10:23:18 AM
 Viewed: 11/30/2018 11:22:50 AM
 Signed: 11/30/2018 11:22:57 AM

Electronic Record and Signature Disclosure:

Not Offered via DocuSign

In Person Signer Events

Signature

Timestamp

Editor Delivery Events

Status

Timestamp

Agent Delivery Events

Status

Timestamp

Intermediary Delivery Events

Status

Timestamp

Certified Delivery Events

Status

Timestamp

ELECTRONIC RECORD AND SIGNATURE DISCLOSURE

From time to time, Transamerica Procurement (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through your DocuSign, Inc. (DocuSign) Express user account. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to these terms and conditions, please confirm your agreement by clicking the 'I agree' button at the bottom of this document.

Getting paper copies

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. For such copies, as long as you are an authorized user of the DocuSign system you will have the ability to download and print any documents we send to you through your DocuSign user account for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a \$0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

Withdrawing your consent

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

Consequences of changing your mind

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. To indicate to us that you are changing your mind, you must withdraw your consent using the DocuSign 'Withdraw Consent' form on the signing page of your DocuSign account. This will indicate to us that you have withdrawn your consent to receive required notices and disclosures electronically from us and you will no longer be able to use your DocuSign Express user account to receive required notices and consents electronically from us or to sign electronically documents from us.

All notices and disclosures will be sent to you electronically

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through your DocuSign user account all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

How to contact Transamerica Procurement:

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:

To contact us by email send messages to: procurement@transamerica.com

To advise Transamerica Procurement of your new e-mail address

To let us know of a change in your e-mail address where we should send notices and disclosures electronically to you, you must send an email message to us at procurement@transamerica.com and in the body of such request you must state: your previous e-mail address, your new e-mail address. We do not require any other information from you to change your email address..

In addition, you must notify DocuSign, Inc to arrange for your new email address to be reflected in your DocuSign account by following the process for changing e-mail in DocuSign.

To request paper copies from Transamerica Procurement

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an e-mail to procurement@transamerica.com and in the body of such request you must state your e-mail address, full name, US Postal address, and telephone number. We will bill you for any fees at that time, if any.

To withdraw your consent with Transamerica Procurement

To inform us that you no longer want to receive future notices and disclosures in electronic format you may:

- i. decline to sign a document from within your DocuSign account, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;
- ii. send us an e-mail to procurement@transamerica.com and in the body of such request you must state your e-mail, full name, IS Postal Address, telephone number, and account number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

Required hardware and software

Operating Systems:	Windows2000? or WindowsXP?
Browsers (for SENDERs):	Internet Explorer 6.0? or above
Browsers (for SIGNERS):	Internet Explorer 6.0?, Mozilla FireFox 1.0, NetScape 7.2 (or above)
Email:	Access to a valid email account
Screen Resolution:	800 x 600 minimum
Enabled Security Settings:	• Allow per session cookies

- | | |
|--|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <ul style="list-style-type: none">• Users accessing the internet behind a Proxy Server must enable HTTP 1.1 settings via proxy connection |
|--|---------------------------------------------------------------------------------------------------------------------------------------------------------|

** These minimum requirements are subject to change. If these requirements change, we will provide you with an email message at the email address we have on file for you at that time providing you with the revised hardware and software requirements, at which time you will have the right to withdraw your consent.

Acknowledging your access and consent to receive materials electronically

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please verify that you were able to read this electronic disclosure and that you also were able to print on paper or electronically save this page for your future reference and access or that you were able to e-mail this disclosure and consent to an address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format on the terms and conditions described above, please let us know by clicking the 'I agree' button below.

By checking the 'I Agree' box, I confirm that:

- I can access and read this Electronic CONSENT TO ELECTRONIC RECEIPT OF ELECTRONIC RECORD AND SIGNATURE DISCLOSURES document; and
- I can print on paper the disclosure or save or send the disclosure to a place where I can print it, for future reference and access; and
- Until or unless I notify Transamerica Procurement as described above, I consent to receive from exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to me by Transamerica Procurement during the course of my relationship with you.

Change Order No. 3 to Statement of Work LTC Drop Ticket process

This Change Order No. 3 ("Change Order") is dated as of January 24, 2019 ("Execution Date"), and is by and between Money Services, Inc. ("MSI") and Examination Management Services, Inc. ("Consultant"). This Change Order is incorporated into that certain Statement of Work LTC Drop Ticket process dated October 12, 2017, Change Order No. 1 dated February 16, 2018, and Change Order No. 2 dated October 26, 2018 (as amended, "SOW") to the Professional Services Agreement dated April 1, 2014 ("Agreement"), between Consultant and MSI. The terms and conditions that are specific to this Change Order are set forth below. In the event of a conflict between the provisions of this Change Order and any prior change order, the provisions of this Change Order shall control such conflict. In the event of a conflict between the provisions of this Change Order and the SOW, the provisions of this Change Order will control such conflict. In the event of a conflict between the provisions of this Change Order and the Agreement, the provisions of the Agreement will control unless the specific provision of the Agreement is identified as superseded.

1.0 Change Summary:

Updating the pricing structure to add additional fees and costs associated with Consultant's use of licensed agents as Application Specialists.

2.0 Licensed Agents: The parties agree that Consultant shall take steps towards using licensed insurance agents as Application Specialists hereunder within ninety (90) days after the Execution Date. For clarity, each Application Specialist who works hereunder shall have at least ninety (90) days from the Execution Date to obtain an insurance license. In connection therewith, MSI agrees to reimburse Consultant any life agent and/or long term care agent licensing fees for Application Specialists who perform Services under the SOW and any costs associated with obtaining and maintaining such licenses by Application Specialist such as, without limitation, educational or study materials.

3.0 Sections of the SOW modified by this Change Order:

3.1 **Section 7 of the SOW is hereby deleted in its entirety and replaced by the following:**

"7.0 Fees:

MSI will pay Consultant for the Services and Deliverables hereunder on an hourly basis as set forth in the table below. Consultant will submit the hours worked for each Application Specialist on a weekly basis and invoices to MSI on a monthly basis. In addition to the hourly rate below, MSI will pay \$2.65 per minute for any Application Specialist's use of the language line. Any script or form changes will be billed to MSI at \$125.00 per hour with prior written authorization. MSI also agrees to pay a one-time implementation fee of \$15,900.00 to cover all IT resources needed to initiate the Services (including without limitation, the establishment of desk access to computers, phone lines, monitors, a new 800 number, and email addresses), payable to Consultant up front; however this implementation fee is an estimate only and any requested changes to the scope of any work performed as a part of the implementation services, shall be added to the implementation at the \$125 hourly rate listed above. In the event the parties increased the number of Application Specialists hereunder, additional implementation fees will apply.

Consultant will immediately notify MSI in writing as soon as Consultant becomes aware that any of the estimated fees under this SOW may exceed any estimated amounts set forth herein. Under no circumstances may any fees under this SOW exceed the estimated or specified amounts provided herein without the prior written consent of both Parties via an amendment or Change Order to this SOW.

It is estimated that each Application Specialist will work approximate forty (40) hours per week. While on the project, MSI will be billed only for actual hours the Application Specialist is engaged in the Services specified in this SOW, or applicable training. MSI will not be billed for any time taken off for personal reasons, sick leave, vacation time, etc.

Role	Number of Application Specialists**	Hourly Rate (0-40 Hours p/week)	Hourly Rate (Hours worked p/week greater than 45 hours)*	Hourly Rate While in Training	Hourly Rate for Application Specialist study time in connection with life agent and/or long term care agent licensing testing to meet MSI licensed agent requirements	Packet Mailing
Application Specialist		\$32.50	\$48.75	\$32.50	\$28.00	\$12.00 per packet mailed for standard two (2) day shipping. Overnight shipping allowed with approval by MSI, and will be passed through at cost.

* MSI must give written approval prior to any Application Specialist billing greater than forty (40) hours in any one week.

* MSI must give approval prior to any additional Application Specialist being added.

- Training is expected to take place in Hewitt or Waco, TX in the first 2-3 weeks of a new Application Specialist being added to the engagement. MSI will provide the trainer(s) and training will be done one-on-one using remote desktop sharing.

Travel and expenses for each Application Specialist who works hereunder (expressly including, but not limited to, life agent and/or long term care agent licensing fees for Application Specialists and any costs associated with obtaining and maintaining such licenses by Application Specialist such as, without limitation, educational or study materials) are not included in the fees set forth above, and will be billed at cost to MSI by Consultant. All travel expenses will comply with the PSA and Exhibit A: Travel Expense Policy in the SOW. Itemized expense reports will be provided with expense invoices and receipts. Consultant will make every effort to ensure travel expenses are reasonable or get approval prior to booking unusually expensive airfare/hotels (e.g. last minute airfare, airline rerouting, and hotel bookings during events)."

**Consultant may add two (2) additional Application Specialists with MSI approval. If additional Application Specialists are needed after that an updated Change Order will be required.

THE PARTIES ACKNOWLEDGE THAT THEY HAVE READ THIS CHANGE ORDER, UNDERSTAND IT, AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS. FURTHER, THE PARTIES AGREE THAT THE COMPLETE AND EXCLUSIVE STATEMENT OF THE AGREEMENT BETWEEN THE PARTIES RELATING TO THIS SUBJECT SHALL CONSIST OF 1) THIS CHANGE ORDER, 2) PRIOR CHANGE ORDERS, IF ANY, 3) THE SOW, AND 4) THE AGREEMENT (INCLUDING THE EXHIBITS THERETO), INCLUDING THOSE CHANGE ORDERS MADE EFFECTIVE BY THE PARTIES IN THE FUTURE. THIS STATEMENT OF THE CHANGE ORDER BETWEEN THE PARTIES SUPERSEDES ALL PROPOSALS OR OTHER PRIOR AGREEMENTS, ORAL OR WRITTEN, AND ALL OTHER COMMUNICATIONS BETWEEN THE PARTIES RELATING TO THE SUBJECT DESCRIBED HEREIN.

[Signature Page to Follow]

PROFESSIONAL SERVICES WORK ORDER

REQUEST #: CR3494 Transamerica Form Update FL Posting

<i>Internal EMSI Use Only</i>	
Division	Percentage
Premier Solutions	100

EMSI shall be excused and not be liable for any failure of or delay in the performance of this Work Order to the extent such failure or delay is due to Client or any third parties or any causes beyond its reasonable control, including but not limited to acts of God, war, strikes or labor disputes, embargoes, government orders or any other force majeure events or circumstances.

- After considering the time and cost impacts provided by EMSI for the requested modification, **Money Services, Inc.** wishes to pursue this request with a complete understanding of the additional time and costs associated with implementing the request.
- After considering the time and cost impacts provided by EMSI for the requested modification, **Money Services, Inc.** wishes to withdraw the request.

AUTHORIZATION:

Money Services, Inc.	Examination Management Services, Inc. – Joe Dickman
Michael Nacarato <small>(Signature)</small> Michael Nacarato	 <small>(Signature)</small> Joe Dickman
Vice President 5/26/2020 <small>(Date)</small>	Vice President – IT Professional Services May 22, 2020 <small>(Date)</small>

SM BH



Certificate Of Completion

Envelope Id: 956A50ECD7B74187842284FA37031C65
 Subject: CW2330001 - CR3494 Transamerica SOW 18_May2020_JD.signed.pdf
 Source Envelope:
 Document Pages: 3 Signatures: 1
 Certificate Pages: 5 Initials: 2
 AutoNav: Enabled
 Enveloped Stamping: Enabled
 Time Zone: (UTC-06:00) Central Time (US & Canada)

Status: Completed
 Envelope Originator:
 DeAnn Kotlarz
 6400 C St. SW
 Cedar Rapids, IA 52499
 DeAnn.Kotlarz@transamerica.com
 IP Address: 216.109.110.11

Record Tracking

Status: Original	Holder: DeAnn Kotlarz	Location: DocuSign
5/26/2020 12:19:45 PM	DeAnn.Kotlarz@transamerica.com	

Signer Events

Linda McFadden		Timestamp
Linda.McFadden@transamerica.com		Sent: 5/26/2020 12:22:05 PM
Lead Vendor Manager		Viewed: 5/26/2020 12:31:01 PM
Underwriting - Vendor Management		Signed: 5/26/2020 12:31:13 PM
Security Level: Email, Account Authentication (None)	Signature Adoption: Pre-selected Style Using IP Address: 198.39.4.71	

Electronic Record and Signature Disclosure:

Accepted: 10/2/2018 10:10:53 AM
ID: 680b8712-737d-43a7-8486-958a8b90c423

Brian Haroldson
Brian.Haroldson@transamerica.com
Transamerica Procurement
Security Level: Email, Account Authentication (None)

Signature Adoption: Pre-selected Style
Using IP Address: 198.39.4.65

Electronic Record and Signature Disclosure:

Not Offered via DocuSign

Michael Nacarato
michael.nacarato@transamerica.com
Vice President
Security Level: Email, Account Authentication (None)

Signature Adoption: Pre-selected Style
Using IP Address: 198.39.4.64

Electronic Record and Signature Disclosure:

Accepted: 9/26/2018 11:00:04 AM
ID: 10d3daab-94ae-4b7c-aaa6-5dc725b100f6

In Person Signer Events

Signature

Editor Delivery Events

Status

Agent Delivery Events

Status

Intermediary Delivery Events

Status

Certified Delivery Events

Status



Certificate Of Completion

Envelope Id: 3004BA24654F4B7291F15B0E71E70B69 Status: Completed
 Subject: CW2333860 - CR3516 Transamerica 103 Updates for Posting SOW v1.1 Clean_JD_signed.pdf
 Source Envelope:
 Document Pages: 3 Signatures: 1 Envelope Originator:
 Certificate Pages: 5 Initials: 2 DeAnn Kotlarz
 AutoNav: Enabled 6400 C St. SW
 EnvelopeId Stamping: Enabled Cedar Rapids, IA 52499
 Time Zone: (UTC-06:00) Central Time (US & Canada) DeAnn.Kotlarz@transamerica.com
 IP Address: 216.109.110.11

Record Tracking

Status: Original	Holder: DeAnn Kotlarz	Location: DocuSign
5/29/2020 2:05:12 PM	DeAnn.Kotlarz@transamerica.com	

Signer Events

Linda McFadden	Signature	Timestamp
Linda.McFadden@transamerica.com		Sent: 5/29/2020 2:07:23 PM
Lead Vendor Manager		Viewed: 5/29/2020 2:09:17 PM
Underwriting - Vendor Management		Signed: 5/29/2020 2:09:25 PM
Security Level: Email, Account Authentication (None)	Signature Adoption: Pre-selected Style Using IP Address: 198.39.4.74	

Electronic Record and Signature Disclosure:

Accepted: 10/2/2018 10:10:53 AM
 ID: 680b8712-737d-43a7-8486-958a8b90c423

Brian Haroldson
 Brian.Haroldson@transamerica.com
 Transamerica Procurement
 Security Level: Email, Account Authentication (None)

Sent: 5/29/2020 2:09:26 PM
 Viewed: 5/29/2020 2:43:14 PM
 Signed: 5/29/2020 2:43:23 PM

Electronic Record and Signature Disclosure:

Not Offered via DocuSign

Michael Nacarato
 michael.nacarato@transamerica.com
 Vice President
 Security Level: Email, Account Authentication (None)

Sent: 5/29/2020 2:43:24 PM
 Viewed: 5/29/2020 2:48:47 PM
 Signed: 5/29/2020 2:49:03 PM

Signature Adoption: Pre-selected Style
Using IP Address: 198.39.4.78

Electronic Record and Signature Disclosure:

Accepted: 9/26/2018 11:00:04 AM
 ID: 10d3daab-94ae-4b7c-aaa6-5dc7253100f6

In Person Signer Events

Signature

Timestamp

Editor Delivery Events

Status

Timestamp

Agent Delivery Events

Status

Timestamp

Intermediary Delivery Events

Status

Timestamp

Certified Delivery Events

Status

Timestamp

Carbon Copy Events	Status	Timestamp
Witness Events	Signature	Timestamp
Notary Events	Signature	Timestamp
Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	5/29/2020 2:43:24 PM
Certified Delivered	Security Checked	5/29/2020 2:48:47 PM
Signing Complete	Security Checked	5/29/2020 2:49:03 PM
Completed	Security Checked	5/29/2020 2:49:03 PM
Payment Events	Status	Timestamps
Electronic Record and Signature Disclosure		

ELECTRONIC RECORD AND SIGNATURE DISCLOSURE

From time to time, Transamerica Procurement (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through your DocuSign, Inc. (DocuSign) Express user account. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to these terms and conditions, please confirm your agreement by clicking the 'I agree' button at the bottom of this document.

Getting paper copies

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. For such copies, as long as you are an authorized user of the DocuSign system you will have the ability to download and print any documents we send to you through your DocuSign user account for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a \$0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

Withdrawing your consent

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

Consequences of changing your mind

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. To indicate to us that you are changing your mind, you must withdraw your consent using the DocuSign 'Withdraw Consent' form on the signing page of your DocuSign account. This will indicate to us that you have withdrawn your consent to receive required notices and disclosures electronically from us and you will no longer be able to use your DocuSign Express user account to receive required notices and consents electronically from us or to sign electronically documents from us.

All notices and disclosures will be sent to you electronically

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through your DocuSign user account all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

How to contact Transamerica Procurement:

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:

To contact us by email send messages to: procurement@transamerica.com

To advise Transamerica Procurement of your new e-mail address

To let us know of a change in your e-mail address where we should send notices and disclosures electronically to you, you must send an email message to us at procurement@transamerica.com and in the body of such request you must state: your previous e-mail address, your new e-mail address. We do not require any other information from you to change your email address..

In addition, you must notify DocuSign, Inc to arrange for your new email address to be reflected in your DocuSign account by following the process for changing e-mail in DocuSign.

To request paper copies from Transamerica Procurement

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an e-mail to procurement@transamerica.com and in the body of such request you must state your e-mail address, full name, US Postal address, and telephone number. We will bill you for any fees at that time, if any.

To withdraw your consent with Transamerica Procurement

To inform us that you no longer want to receive future notices and disclosures in electronic format you may:

- i. decline to sign a document from within your DocuSign account, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;
- ii. send us an e-mail to procurement@transamerica.com and in the body of such request you must state your e-mail, full name, IS Postal Address, telephone number, and account number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

Required hardware and software

Operating Systems:	Windows2000? or WindowsXP?
Browsers (for SENDERs):	Internet Explorer 6.0? or above
Browsers (for SIGNERS):	Internet Explorer 6.0?, Mozilla FireFox 1.0, NetScape 7.2 (or above)
Email:	Access to a valid email account
Screen Resolution:	800 x 600 minimum
Enabled Security Settings:	<ul style="list-style-type: none">• Allow per session cookies

- | | |
|--|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| | <ul style="list-style-type: none">• Users accessing the internet behind a Proxy Server must enable HTTP 1.1 settings via proxy connection |
|--|---------------------------------------------------------------------------------------------------------------------------------------------------------|

** These minimum requirements are subject to change. If these requirements change, we will provide you with an email message at the email address we have on file for you at that time providing you with the revised hardware and software requirements, at which time you will have the right to withdraw your consent.

Acknowledging your access and consent to receive materials electronically

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please verify that you were able to read this electronic disclosure and that you also were able to print on paper or electronically save this page for your future reference and access or that you were able to e-mail this disclosure and consent to an address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format on the terms and conditions described above, please let us know by clicking the 'I agree' button below.

By checking the 'I Agree' box, I confirm that:

- I can access and read this Electronic CONSENT TO ELECTRONIC RECEIPT OF ELECTRONIC RECORD AND SIGNATURE DISCLOSURES document; and
- I can print on paper the disclosure or save or send the disclosure to a place where I can print it, for future reference and access; and
- Until or unless I notify Transamerica Procurement as described above, I consent to receive from exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to me by Transamerica Procurement during the course of my relationship with you.

Exhibit C

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (“Agreement”) is entered into as of September 24, 2014 (the “Effective Date”), by and between **Examination Management Services, Inc.** (“BA”) and **TRANSAMERICA LIFE INSURANCE COMPANY** an Iowa corporation, on behalf of the Covered Entity, which are the health care components of Transamerica Life Insurance Company, Transamerica Financial Life Insurance Company, Transamerica Premier Life Insurance Company, Stonebridge Life Insurance Company, and Western Reserve Life Assurance Company Co. of Ohio.

WHEREAS, the above listed entities, excepting BA, have elected to adopt Affiliated Covered Entity status, as defined and permitted under the Health Insurance Portability and Accountability Act of 1996 and its rules and regulations (as any of the same may be amended or superseded from time to time, “HIPAA”), such designation has been appropriately adopted and documented, and the Covered Entity (as defined below) is authorized to enter into a Business Associate Agreement.

WHEREAS, Covered Entity and BA have or will entered into a services agreement under which BA is providing certain specified services to the Covered Entity (the “Service Agreement”), and during the course and scope of providing Services (as defined below) under the Service Agreement, the BA will have access to Protected Health Information (as defined below);

WHEREAS, BA is considered a “Business Associate” as defined in 45 CFR 160.103, as may be amended and/or superseded from time to time;

WHEREAS, Pursuant to HIPAA, BA and Covered Entity desire to execute this Agreement to comply with the terms of 45 CFR 160-164 including but not limited to the Privacy Rule, Security Rule, and Breach Notification Rule issued under HIPAA and the HITECH Act (each as defined below, and as amended and/or superseded from time to time, collectively, referred to herein as the “HIPAA Rules”).

WHEREAS, Covered Entity and BA wish to (as applicable) either modify the Service Agreement or update the existing Business Associate Agreement between them to include certain provisions required by the HIPAA Rules.

WHEREAS, to the extent the Service Agreement either embedded the obligations of a Business Associate in its terms and conditions, or addressed such obligations via an amendment, exhibit, appendix, addendum, attachment or standalone agreement, this Agreement will be deemed to replace such terms and conditions related to the obligations of BA as a Business Associate in its entirety. No other terms and conditions of the Service Agreement shall be deemed impacted by this Agreement.

NOW, THEREFORE, in consideration of the mutual covenants, terms and conditions herein contained, and the provision, or continued provision of Protected Health Information by Covered Entity to BA under the Service Agreement in reliance of this Agreement, the parties hereto agree as follows:

Section 1: Definitions

Terms used but not otherwise defined in this Agreement shall have the same meaning as those terms in the HIPAA Rules. To the extent any of the statutory references applicable to the terms defined below are updated, amended or superseded from time to time, such updated, amended or superseded statutory references shall apply to such defined term. To the extent any of the defined terms have any regulations promulgated, the defined term shall apply to any applicable regulations promulgated thereunder as they become effective.

- (a) **Breach** shall mean either the reasonable suspicion or actual acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under the Privacy Rule which compromises the security or privacy of the Protected Health Information, as defined in 45 CFR § 164.402.
- (b) **Breach Notification Rule** shall mean that portion of the HIPAA Rules set forth in 45 CFR Part 160 and in subparts A and D of 45 CFR Part 164.
- (c) **Covered Entity** shall mean individually and collectively, the health care components of the following entities:

- TRANSAMERICA LIFE INSURANCE COMPANY
- TRANSAMERICA FINANCIAL LIFE INSURANCE COMPANY
- TRANSAMERICA PREMIER LIFE INSURANCE COMPANY
- STONEBRIDGE LIFE INSURANCE COMPANY
- WESTERN RESERVE LIFE ASSURANCE CO. OF OHIO

The Covered Entity list may be amended or modified from time to time by notice to BA of such change to the Covered Entity listing. Such notice will be treated as an addendum to this Amendment. This Agreement will continue to apply to the health care components of the Covered Entity in the event of a merger or name change involving any of the entities.

(d) **Data Aggregation** shall mean, with respect to Protected Health Information created or received by BA in its capacity as a business associate of Covered Entity, the combining of such Protected Health Information by BA with the Protected Health Information received by BA in its capacity as a business associate of another covered entity, to permit data analyses that relate to the Health Care Operations (defined below) of the respective covered entities. The meaning of "data aggregation" in this Agreement shall be consistent with the meaning given to that term in the Privacy Rule.

(e) **Designated Record Set** shall mean a group of Records maintained by or for the Covered Entity that: consists of (i) medical records and billing records about Individuals maintained by or for the Covered Entity; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) Records used, in whole or in part, by or for the Covered Entity to make decisions about Individuals. For purposes of this definition, the term "Record" means any item, collection, or grouping of information that includes Protected Health Information and is maintained, collected, used, or disseminated by or for the Covered Entity. The term "Designated Record Set", however, shall not include any information in the possession of BA that: (i) is the same as information in the possession of Covered Entity (information shall be considered the same information even if the information is held in a different format, medium or presentation or it has been standardized); (ii) is

compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding, including but not limited to, any information subject to the attorney-client privilege, trial preparation immunity, attorney work product, peer review privilege or other privilege under applicable law; or (iii) constitutes “psychotherapy notes” as defined in 45 CFR § 164.501.

(f) “**De-Identify**” shall mean to alter the Protected Health Information such that the resulting information meets the requirements described in 45 CFR § 164.514(a), (b), (c).

(g) “**Electronic Health Record**” shall have the same meaning as the term “electronic health record” in Section 13400(5) of the HITECH Act.

(h) “**Electronic Protected Health Information**” shall have the same meaning as the term “electronic protected health information” in 45 CFR § 160.103, to the extent such Electronic Protected Health Information is information that BA creates, accesses, or receives, maintains, transmits from or on behalf of Covered Entity.

(i) “**Electronic Transaction Rules**” shall mean the final regulations issued by HHS concerning standard transactions and code sets under 45 CFR Parts 160 and 162.

(j) “**Health Care Operations**” shall have the meaning given to that term at 45 CFR. § 164.501.

(k) “**HITECH Act**” shall mean the Health Information Technology for Economic and Clinical Health Act, as incorporated in the American Recovery and Reinvestment Act of 2009, Public Law 111-5.

(l) “**HHS**” shall mean the U.S. Department of Health and Human Services or its designee.

(m) “**Individual**” shall have the same meaning as the term “individual” in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

(n) “**Privacy Rule**” shall mean that portion of the HIPAA Rules set forth in 45 CFR Part 160 and Part 164, subparts A and E.

(o) “**Protected Health Information**” shall mean information transmitted or maintained in any form or medium, including demographic information collected from an Individual that has the same meaning as the term “protected health information” in 45 CFR § 160.103 and/or the HIPAA Rules, and:

- i. is created or received by Covered Entity; and
- ii. relates to the past, present, or future physical or mental health or condition of an Individual; the provision of health care to an Individual; or the past, present, or future payment for the provision of health care to an Individual, and (a) identifies the Individual or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the Individual;

Protected Health Information is limited to the information created or received by the BA from or on behalf of the Covered Entity in connection with the Services.

(p) “**Required By Law**” shall have the same meaning as the term “required by law” in 45 CFR § 164.103.

(q) “**Secretary**” shall mean the Secretary of the U.S. Department of Health and Human Services or his or her designee.

(r) “**Security Incident**” shall mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system as defined in 45 CFR § 164.304. This term shall not include trivial incidents that occur on a daily basis, such as scans, “pings,” or unsuccessful attempts to penetrate computer networks or servers maintained by BA. The term shall be limited to such incidents involving Protected Health Information or information systems containing Electronic Protected Health Information.

(s) “**Security Rule**” shall mean that portion of the HIPAA Rules set forth in 45 CFR Part 160 and Part 164, subparts A and C.

(t) “**Services**” shall mean the services provided by BA to the Covered Entity, as specified in the Service Agreement or contemplated as part of the professional services agreement.

(u) “**Subcontractor**” shall mean means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate

(v) “**Unsecured Protected Health Information**” shall mean Protected Health Information that has not been secured in accordance with the standards promulgated by the Secretary of HHS in guidance issued by the HHS or the Office of Civil Rights (“OCR”) under section 13402(h)(2) of the HITECH Act or 45 CFR 164.402.

Section 2: Obligation and Activities of BA

(a) **BA Obligations.** BA acknowledges and agrees that it is considered a “Business Associate” as defined by the HIPAA Rules. As a Business Associate of Covered Entity, BA agrees that it is directly subject to the HIPAA Rules, including its provisions relating to security and privacy of Protected Health Information as well as its enforcement and penalty provisions. BA agrees that it shall: (i) comply with all applicable security and privacy provisions of the HIPAA Rules, as well as all applicable state and local laws and regulations enacted to protect the privacy and security of Individuals’ Protected Health Information; and (ii) not act in any way to interfere with or hinder Covered Entity’s ability to comply with the HIPAA Rules. To the extent that BA is carrying out Covered Entity’s obligations under the HIPAA Rules as expressly provided herein or through amendment, BA shall comply with the requirements of the HIPAA Rules that apply to Covered Entity in the performance of such obligation.

(b) **Use of Protected Health Information.**

i. BA agrees to not use or disclose Protected Health Information other than as permitted or required by this Agreement, the HIPAA Rules or as Required By Law, and only as reasonably necessary to provide the Services described in the Service Agreement, to or on behalf of the Covered Entity.

- ii. BA shall use or disclose only the minimum necessary amount of Protected Health Information, in accordance with Section 13405(b) the HITECH Act, for each use or disclosure of Protected Health Information hereunder
- iii. BA recognizes that the Protected Health Information is and shall remain the Covered Entity's property except as set forth under the terms of the Service Agreement. BA agrees that it acquires no title or rights to the Protected Health Information as a result of this Agreement.
- iv. Except as otherwise limited by this Agreement, Covered Entity authorizes BA to use and disclose Protected Health Information in its possession for the proper management and administration of BA's business and to carry out its legal responsibilities under the Service Agreement. BA may disclose Protected Health Information for such purposes, provided that (aa) such disclosures are Required By Law; or (bb) BA obtains, in writing, prior to making any disclosure to a third party: (i) reasonable assurances from such third party that the Protected Health Information will be held confidential as provided under this Agreement and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to such third party; and (ii) an agreement from such third party to notify BA immediately of any breaches of the confidentiality of the Protected Health Information, to the extent it has knowledge of such breach and (iii) BA obtains appropriate satisfactory assurances that all Protected Health Information will be handled in accordance with HIPAA Rules and that receipt of such Protected Health Information may subject recipient to Subcontractor obligations.
- v. Absent Covered Entity's prior express written permission, the Covered Entity does not authorize BA to provide Data Aggregation services with respect to the Protected Health Information and does not authorize BA to De-Identify the Protected Health Information.
- vi. Except as permitted under subparagraphs (i-iv) of this section, BA shall not use and/or disclose Protected Health Information in a manner that would violate the HIPAA Rules if done by Covered Entity.
- vii. Upon written request, BA shall make available to Covered Entity any of Covered Entity's Protected Health Information that BA has in its possession.

(c)

Safeguards.

- i. BA represents and warrants that it has implemented and shall maintain reasonable administrative, physical and technical safeguards (the "Safeguards") designed to prevent prohibited uses or disclosures, and to protect the confidentiality, integrity and availability, of Protected Health Information that it creates, receives, maintains or transmits. Such safeguards shall include development, implementation, and maintenance of a comprehensive written information security program Required By Law and designed to: (i) protect the availability, integrity and confidentiality of Protected Health Information, (ii) protect against anticipated threats or hazards to the security, confidentiality and/or integrity of Protected Health Information, (iii) protect against any unauthorized, disclosure, or use of Protected Health Information, (iv) address computer and network security, (v) address physical security, and (vi) provide for the secure destruction and disposal of Protected Health Information. The Safeguards requirement applies equally to Electronic Protected Health Information that the BA creates, receives, maintains, or transmits on behalf of the Covered Entity. At all times, BA Safeguards shall be consistent with the requirements of 45 CFR 164(c)

ii. BA agrees to take reasonable steps and obtain satisfactory assurances to ensure that the actions or omissions of its agents and/or Subcontractors do not cause the BA to breach the terms of this Agreement.

(d) **Mitigation.** BA agrees to mitigate, to the extent practicable, any harmful effect that is known to BA of: (i) a use or disclosure of Protected Health Information by BA or its agents or Subcontractors, in violation of the requirements of this Agreement, or (ii) any Security Incident.

(e) **Reporting; Data Breach.**

i. BA shall report to Covered Entity in writing to both the email and physical addresses set forth in Section 6(i) of this Agreement, and without unreasonably delay, and in no event, within three (3) calendar days of discovery, any use or disclosure of Protected Health Information not permitted or required by this Agreement, and/or any Breach, and/or any Security Incident of which it becomes aware. To the extent BA is reporting discovery of a Breach of Unsecured Protected Health Information, such shall be treated as discovered in accordance with 45 CFR § 164.410(a)(2).

ii. BA shall also require its employees, agents, and Subcontractors to immediately report to BA any use or disclosure of Protected Health Information in violation of this Agreement.

iii. To the extent that BA, exercising reasonable diligence, has knowledge or a reasonable belief that a Breach of Unsecured Protected Health Information of the Covered Entity has occurred, BA shall promptly (but in no event more than three (3) calendar days of knowledge of the Breach or reasonable belief that a Breach of Unsecured Protected Health Information has occurred) notify the Covered Entity, to both the email and physical addresses set forth in Section 6(i) of this Agreement, in accordance with the requirements of 45 CFR § 164.410. Such notification shall include, to the extent possible, the identification of each Individual whose Protected Health Information has been or is reasonably believed to have been accessed, acquired, used or disclosed during the Breach, along with any other information that the Covered Entity will be required to include in its notification to the Individual under the 45 CFR § 164.404(c), including, without limitation, a description of the Breach, the date of the Breach and its discovery, types of Unsecured Protected Health Information involved and description of the BA's investigation, mitigation, and prevention efforts.

iv. At the reasonable direction of Covered Entity, BA shall provide affected Individuals the notice required under 45 CFR § 164.404(c) relating to any Breach by BA. BA shall provide such information as may be necessary for Covered Entity to report a Breach to HHS as required by 45 CFR § 164.408 and shall provide reasonable assistance with such reporting obligation (and, upon Covered Entity's request, and to the extent permitted by law, BA shall submit the necessary report to HHS on behalf of the Covered Entity).

(f) **Agents and Subcontractors.** In accordance with 45 CFR §§ 164.502(e)(1)(ii) and 164.308(b)(2), BA agrees to require that any of its agents and/or Subcontractors to whom it provides Protected Health Information to on behalf of Covered Entity, agree in writing to substantially the same kinds of restrictions and conditions that apply through this Agreement to BA with respect to such information apply to such agents and/or Subcontractors. The BA shall require its agents and/or Subcontractors to agree: (i) in writing to substantially the same kinds of restrictions, conditions, and requirements

concerning the uses and disclosures of Protected Health Information as apply to BA with respect to Protected Health Information and as contained in this Agreement and applicable HIPAA Rules; and (ii) agree in writing to comply with the applicable provisions of the Security Rule with respect to any Electronic Protected Health Information that it creates, receives, maintains or transmits on behalf of BA or Covered Entity.

(g) **Access by Individuals.**

- i. BA agrees to provide access, at the written request of Covered Entity, and upon five (5) business days advance written notice, to Protected Health Information in a Designated Record Set, to Covered Entity or, as reasonably directed by Covered Entity, to an Individual in a form and format order to meet the requirements under 45 CFR § 164.524. BA may charge Covered Entity an agreed upon fee for such info. If the Protected Health Information is held in an Electronic Health Record, then the BA shall provide access to such Electronic Health Records in electronic form if so requested, including transmitting an Electronic Health Record in electronic form to a third party designated by an Individual who is the subject of such Electronic Health Record.
- iii. Any disclosure of, or decision not to disclose, the Protected Health Information requested by an Individual and compliance with the requirements applicable to an Individual's right to obtain access to Protected Health Information shall be the sole responsibility of the Covered Entity.

(h) **Amendments to Protected Health Information.**

- i. BA agrees to make any reasonable amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR § 164.526 at the request of Covered Entity or an Individual, and upon fifteen (15) days advance written notice by Covered Entity. BA may charge Covered Entity a reasonable fee for such amendments.
- ii. In the event that any Individual requests that BA amend such Individual's Protected Health Information or Record in a Designated Record Set, BA shall forward such request within five (5) business days to Covered Entity.
- iii. Any amendment of, or decision not to amend, the Protected Health Information or Record as requested by an Individual and compliance with the requirements applicable to an Individual's right to request an amendment of Protected Health Information shall be the sole responsibility of the Covered Entity.

(i) **Access by Covered Entity and Secretary.** BA agrees to make internal practices, books and records including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, or created or received by BA on behalf of, Covered Entity available to the Covered Entity, with 30 days advance written notice by the Covered Entity or the Secretary in a time and manner designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the HIPAA Rules. Covered Entity agrees to pay BA's then-current cost of supporting any such access requested by the Covered Entity or the Secretary. Notwithstanding the foregoing, prior to any such disclosure to the Secretary, or any other federal or state agency, BA shall notify Covered Entity in writing of such request and shall furnish Covered Entity with copies of such request. BA agrees to reasonably assist Covered Entity's efforts in responding to any such request, including

but not limited to engaging in an effort to obtain a confidentiality agreement, protective order, injunction or court order, if necessary, to preserve any applicable privilege.

(j) **Disclosure Documentation.**

- i. BA agrees to document any such disclosures of Protected Health Information and information related to such disclosures made by BA to the extent that the Covered Entity would be obligated to account for such disclosures under 45 CFR § 164.528. Upon request, BA also shall make available information related to such disclosures as would be required for Covered Entity to respond to a request for an accounting of disclosures in accordance with 45 CFR. § 164.528.
- ii. At a minimum, BA shall furnish Covered Entity the following with respect to any covered disclosures by BA: (i) the date of disclosure of Protected Health Information; (ii) the name of the entity or person who received Protected Health Information, and, if known, the address of such entity or person; (iii) a brief description of the Protected Health Information disclosed; and (iv) a brief statement of the purpose of the disclosure which includes the basis for such disclosure.
- iii. BA agrees to provide to Covered Entity or an Individual, upon thirty (30) days advance written notice by Covered Entity, information collected in accordance with this Subsection (j) to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR § 164.528, or in the event that Covered Entity elects to provide an Individual with a list of its BAs, BA will provide an accounting of its disclosures of Protected Health Information upon request of the Individual, if and to the extent required under Section 13405(c) of the HITECH Act and any regulations adopted thereunder. BA may charge Covered Entity a reasonable fee for such documentation.
- iv. In the event that an Individual delivers the request for an accounting directly to BA, BA shall forward such request promptly to Covered Entity, but in no event, within five (5) business days.
- v. BA hereby agrees to implement a commercially reasonable recordkeeping system to enable it to comply with the requirements of this Section. BA agrees to retain such records for a minimum of six (6) years.
- vi. Unless Covered Entity provides the Individual with a list of business associates as provided in subsection iii. above, Covered Entity shall maintain responsibility for preparing and delivering any accounting requested and for complying with the requirements applicable to an Individual's right to obtain an accounting of disclosures of Protected Health Information.
- vii. The obligations of this section shall apply to all amendments, updates, and further regulations adopted in reference to any of the laws or regulations cited herein.

(k) **Training.** BA agrees to train its employees who handle Covered Entity's Protected Health Information about the BA's obligations and permitted uses and disclosures under this Agreement and the HIPAA Rules.

(l) **Covered Electronic Transactions.** In the event that BA transmits or receives any electronic transaction (within the meaning of 45 CFR § 162, as amended by the Affordable Care Act and its operating rules) on behalf of the Covered Entity, it shall

comply with all applicable provisions of the Electronic Transactions Rules, and shall ensure that any agents or Subcontractors that assist BA in conducting such electronic transactions on behalf of the Covered Entity agree in writing to comply with the Electronic Transactions Rules. BA also shall comply with the National Provider Identifier (as defined in 45 CFR § 162.406) requirements, if and to the extent applicable.

(m) **Prohibition on Sale of Records.** BA shall not directly or indirectly receive remuneration in exchange for any Protected Health Information of an Individual unless the Covered Entity obtained from the Individual, in accordance with 45 CFR § 164.508, a valid authorization that includes a specification of whether the Protected Health Information can be further exchanged for remuneration by the entity receiving Protected Health Information of that Individual, except as otherwise allowed under the HIPAA Rules.

Section 3: Obligations of Covered Entity

(a) **Change in Privacy Practices.** Covered Entity shall promptly notify BA in writing of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR § 164.520, to the extent that such limitation may affect BA's use or disclosure of Protected Health Information.

(b) **Change in right to use Protected Health Information.** Covered Entity shall promptly notify BA in writing of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect BA's use and disclosure of Protected Health Information.

(c) **Change in Restrictions Regarding Protected Health Information.** Covered Entity shall promptly notify BA in writing of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect BA's use or disclosure of Protected Health Information. BA will implement a similar restriction provided such restriction is reasonable and does not impact its ability to perform under the terms of the Service Agreement.

(d) **Covered Entity Representative.** Covered Entity shall notify BA of those employees of Covered Entity who are authorized to receive Protected Health Information from BA.

Section 4: Permissible Requests by Covered Entity

Covered Entity shall not request BA to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity. A written request by an authorized representative of the Covered Entity will be necessary for BA to disclose Protected Health Information of the Covered Entity to a third party unless otherwise expressly permitted under this Agreement.

Section 5: Term and Termination

(a) **Term.** This Agreement will begin on the Effective Date, and will continue until terminated in accordance herein.

(b) **Termination for Cause.** Upon Covered Entity's knowledge of a material breach of this Agreement or pattern or practice in violation of the HIPAA Rules by BA, Covered Entity shall provide not less than thirty (30) calendar day's written notice of its intent to terminate the Service Agreement and this Agreement. If BA does not cure the breach within such time, then Covered Entity may, in its sole discretion, immediately terminate the Service Agreement and this Agreement.

(c) **Termination of the Service Agreement.** This Agreement will immediately terminate if the Service Agreement terminates. The effective date of such termination will be the same as the effective date that the Service Agreement terminates.

(d) **Effect of Termination.**

i. Except as provided in the next paragraph, upon request for any reason, BA shall return or securely destroy (if feasible, as mutually determined by the parties) or securely archive all Protected Health Information received from the Covered Entity, or created or received by BA on behalf of Covered Entity in a commercially reasonable secure manner. If the Protected Health Information is destroyed, BA shall provide Covered Entity with reasonably appropriate evidence of the secure manner of destruction upon request. This provision shall apply to Protected Health Information that is in the possession of Subcontractors or agents of BA. BA shall retain no copies of the Protected Health Information, except in cases of actual or threatened litigation or if Required By Law, or as may be allowed under (ii) below. This provision shall apply to Protected Health Information retained by the Business Associate is subject to record retention requirements provided under the HIPAA Rules as needed to support appropriate evidence of compliance.

ii. In the event that BA determines that returning or destroying the Protected Health Information is infeasible, BA shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon BA's determination that return or destruction of Protected Health Information is infeasible, BA shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as BA maintains such Protected Health Information.

Section 6: Miscellaneous

(a) **Regulatory References.** Any reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended and/or superseded from time to time.

(b) **Amendment.** The Parties agree to take such action as is reasonably necessary to amend this Agreement from time to time as is necessary for the parties to comply with the requirements of the HIPAA Rules, as amended, and to the extent such amendment does not constitute a material change to BA's obligations under this Agreement. Upon the applicable effective date of any amendment to the regulations promulgated by HHS with respect to PHI and any material change to BA's obligations hereunder, this Agreement shall automatically amend such that the obligations imposed on BA as a Business Associate remain in

compliance with such regulations. The parties acknowledge that the HIPAA Rules include provisions that require significant changes as well as provisions regarding promulgation of related rules. The HIPAA Rules may be further clarified in forthcoming regulations and/or guidance by HHS or OCR. Each Party agrees to comply with the applicable provisions of the HIPAA Rules and any implementation regulations issued thereunder. To the extent they are unclear, the terms of this Agreement shall be construed to allow for compliance by Covered Entity and BA with the HIPAA Rules.

(c) **Survival.** The respective rights and obligations of BA under Subsection 5(d) and 6(o) below shall survive the termination of this Agreement.

(d) **Interpretation; Conflict.** Any ambiguity in this Agreement shall be resolved to permit the parties to comply with the HIPAA Rules. In addition, to the extent this Agreement, only as it relates to the HIPAA Rules and Protected Health Information, is inconsistent with the terms of the Service Agreement, the terms of this Agreement shall govern. To the extent the terms of the Service Agreement conflict with the terms of this Agreement unrelated to the HIPAA Rules and Protected Health Information, the terms of the Service Agreement shall govern. All terms of the Service Agreement not in conflict with this Agreement remain in full force and effect.

(e) **No Third-Party Beneficiaries.** Except as expressly provided for in the HIPAA Rules or otherwise specifically set forth in this Agreement, this Agreement is entered into by and among the parties hereto solely for their benefit. Unless otherwise specifically set forth in this Agreement, the parties have not created or established any third-party beneficiary status or rights in any person or entity not a party hereto including, but not limited to, any Individual, provider, Subcontractor, or other third-party, and no such third-party will have any right to enforce any right or enjoy any benefit created or established under this Agreement.

(f) **Force Majeure.** The obligations of any party under this Agreement will be suspended for the duration of any force majeure applicable to that party. The term "force majeure" means any cause not reasonably within the control of the party claiming suspension, including, without limitation, an act of God, industrial disturbance, war, riot, weather-related disaster, earthquake and governmental action. The party claiming suspension under this Subsection (f) will take reasonable steps to resume performance as soon as possible without incurring unreasonably excessive costs.

(g) **Entire Agreement; Amendments; Facsimile.** This Agreement, including any riders, attachments or amendments hereto, constitutes the entire agreement among the parties with respect to the HIPAA Rules. This Agreement supersedes any prior agreement or understandings pertaining to the services provided hereunder, whether oral or written, and may be amended only by a writing executed by authorized representatives of both parties. A facsimile or other reproductive type copy of this Agreement, so long as signed by all parties, will be considered an original and will be fully enforceable against all parties.

(h) **Choice of Law.** This Agreement is made in and will be governed by, and construed in accordance with, the laws of the State of Iowa without regard to principles of conflict or choice of law.

(i) **Assignment and Delegation.** No party may assign its rights or duties under this Agreement without the prior written consent of the other, which consent shall not be unreasonably withheld. This Agreement is binding upon and will inure to the benefit of the respective parties hereto and their successors and permitted assigns.

(j) **Headings.** All headings are for convenience only and may not be deemed to limit, define or restrict the meaning or contents of the Sections.

(k) **Unenforceable Provisions.** If any provision of this Agreement is held to be illegal or unenforceable by a court of competent jurisdiction, the remaining provisions will remain in effect and the illegal or unenforceable provision will be modified so as to conform to the original intent of this Agreement to the greatest extent legally permissible. Notwithstanding the foregoing, if any such modification causes a material change in the obligations or rights of any party, upon written notice from one party to the other of the adverse effect thereof upon such notifying party, and then if the parties are not able to mutually agree as to an amendment hereto, any party may terminate this Agreement upon 30 days written notice to the other parties.

(l) **Notices.**

i. **Generally.** Any notice required pursuant to this Agreement (except for those required under Section 2(e) of this Agreement must be in writing and sent by registered or certified mail, return receipt requested, by fax with proof of delivery, or by a nationally recognized private overnight carrier with proof of delivery, to the addresses of the parties set forth below in this Agreement. The date of notice will be the date on which the recipient receives notice or refuses delivery. All notices must be addressed as follows or to such other address as a party may identify in a notice to the other party:

To Covered Entity:
L&P HIPAA Privacy Official
Attn: Stephanie Eades
4333 Edgewood Rd NE
Cedar Rapids, Iowa 52499

To BA:
EMSI
Attn: General Counsel
3050 Regent Blvd, Suite 400
Irving, TX 75063

ii. **Notices Under Section 2(e).** Any notice or reporting required under Section 2(e) of this agreement shall be made as follows:

tbinformationsecurity@transamerica.com

(m) **Waiver.** A waiver of a breach or default under this Agreement is not a waiver of any other or subsequent breach or default. A failure or delay in enforcing compliance with any term or condition of this Agreement does not constitute a waiver of such term or condition unless it is expressly waived in writing.

(n) **Negotiated Agreement.** Each party acknowledges that this Agreement resulted from negotiations by and among all parties, and therefore any rule of construction requiring ambiguities to be construed against the drafter of an agreement will not apply to any provision of this Agreement.

(o) **Indemnification.** BA shall indemnify and hold harmless Covered Entity, its affiliated companies, their officers, directors, employees, shareholders, successors and assigns, agents and attorneys, from and against any and all liabilities, claims, costs, demands, expenses or loss including but not limited to reasonable attorney's fees and other costs of litigation, incurred by; Covered Entity, its affiliated companies, their officers, directors, employees, shareholders, successors and assigns, as a consequence of any breach of this Agreement including but not limited to any obligations arising under the HIPAA Rules and activities provided for in this Agreement.

(p) **Independent Contractor.** For all purposes hereunder this Agreement, BA's status shall be that of an independent contractor

(q) **Impact on Service Agreement.** To the extent the BA and Covered Entity have already entered into a Service Agreement which has a prior Business Associate Agreement either embedded in its terms and conditions or agreed to via an amendment, exhibit, appendix, attachment or addendum to such Service Agreement, this Agreement will be deemed to replace such terms and conditions related to the obligations of BA as a Business Associate in their entirety, regardless of how it is documented. No other terms and conditions of the Service Agreement shall be deemed impacted by this Agreement.

IN WITNESS WHEREOF, the parties have executed this Agreement the day and date first above written by their duly authorized officers for and on behalf of said entity.

BA

**EXAMINATION MANAGEMENT
SERVICES, INC.**

By: _____

Name: Robert P. Brook

Title: Executive Vice President and CDO

Date: September 29, 2014

COVERED ENTITY

**TRANSAMERICA LIFE INSURANCE
COMPANY, ON BEHALF OF THE
HEALTH CARE COMPONENTS OF ITSELF
AND TRANSAMERICA FINANCIAL LIFE
INSURANCE COMPANY, TRANSAMERICA
PREMIER LIFE INSURANCE COMPANY,
STONEBRIDGE LIFE INSURANCE
COMPANY, AND WESTERN RESERVE LIFE
ASSURANCE CO. OF OHIO**

By: _____

Name: Rob Frederick

Title: Division CEO - EBS

Date: 10/2/14

Exhibit D

From: EMSI Board of Directors [<mailto:board@emsinet.com>]
Sent: Tuesday, August 4, 2020 10:13 AM
To: EMSI Board of Directors <board@emsinet.com>
Subject: EMSI Update [EXTERNAL]

On July 30th, EMSI sold certain of its assets to RDI Xtract. As part of the transaction, RDI Xtract assumed control of the majority of the EMSI IT environment, including the servers and data center housing EMSI's customer data. In addition to hiring several former EMSI employees, RDI Xtract has agreed to maintain, secure and protect all data on the acquired EMSI servers and work with former EMSI customers to determine a solution for their data.

EMSI is in the process of destroying all customer and patient information located in field offices or work stations not acquired by RDI Xtract. This information is likely limited to files processed immediately prior to EMSI's shutdown which may not have been loaded to EMSI's servers.

We thank you for your patience while EMSI personnel worked to address these customer concerns.

Please contact the following individual at RDI Xtract to discuss your data and information requests as EMSI no longer has access to the data nor the servers upon which it is stored:

Kamette Myers, President
RDI Xtract
kmyers@rdixtract.com
(480) 848-1095

Further, if you have specific questions for EMSI, please email them to board@emsinet.com.

Best Regards,

EMSI Board of Directors

Please note: This message originated outside your organization. Please use caution when opening links or attachments.

**FORM NO. 353-3 - CITATION
THE STATE OF TEXAS**

To:

**EMSI HOLDING COMPANY
SERVING ITS REGISTERED AGENT FOR SERVICE
CT CORPORATION 1999 BRYAN STREET, SUITE 900,
DALLAS, TEXAS 75201,**

GREETINGS:

You have been sued. You may employ an attorney. If you or your attorney do not file a written answer with the clerk who issued this citation by 10 o'clock a.m. of the Monday next following the expiration of twenty days after you were served this citation and petition, a default judgment may be taken against you. Your answer should be addressed to the clerk of the **14th District Court** at 600 Commerce Street, Ste. 101, Dallas, Texas 75202.

Said Plaintiff being **MONEY SERVICES, INC.**

Filed in said Court **28th day of August, 2020** against

EXAMINATION MANAGEMENT SERVICES, INC., ET AL

For Suit, said suit being numbered **DC-20-12059**, the nature of which demand is as follows:
Suit on **OTHER (CIVIL)** etc. as shown on said petition, a copy of which accompanies this citation. If this citation is not served, it shall be returned unexecuted.

WITNESS: FELICIA PITRE, Clerk of the District Courts of Dallas, County Texas.
Given under my hand and the Seal of said Court at office this **2nd day of September, 2020**.

ATTEST: FELICIA PITRE, Clerk of the District Courts of Dallas, County, Texas

Courtney Rutledge
By **COURTNEY RUTLEDGE**, Deputy

ESERVE

CITATION

DC-20-12059

MONEY SERVICES, INC.

vs.
**EXAMINATION MANAGEMENT
SERVICES, INC., et al**

ISSUED THIS
2nd day of September, 2020

FELICIA PITRE
Clerk District Courts,
Dallas County, Texas

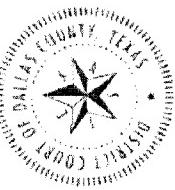
By: COURTNEY RUTLEDGE, Deputy

Attorney for Plaintiff
SUSAN EGELAND
FAEGRE DRINKER BIDDLE & REATH
1717 MAIN STREET SUITE 5400
DALLAS TX 75201-7367
469-357-2533
susan.egeleand@faegredrinker.com

DALLAS COUNTY

SERVICE FEES

NOT PAID



OFFICER'S RETURN

Case No.: DC-20-12059

Court No. 14th District Court

Style: MONEY SERVICES, INC.

vs.

EXAMINATION MANAGEMENT SERVICES, INC., et al

Came to hand on the _____, 20_____, at _____ o'clock _____ M. Executed at _____
within the County of _____ at _____ o'clock _____. M. on the _____ day of _____
20_____, by delivering to the within named _____

each, in person, a true copy of this Citation together with the accompanying copy of this pleading, having first endorsed on same date of delivery. The distance actually traveled by me in serving such process was _____ miles and my fees are as follows: To certify which witness my hand.

For serving Citation \$ _____
For mileage \$ _____ of _____ County, _____
For Notary \$ _____ By _____ Deputy _____

(Must be verified if served outside the State of Texas.)

Signed and sworn to by the said _____ before me this _____ day of _____, 20_____.
to certify which witness my hand and seal of office.

Notary Public _____ County _____

**FORM NO. 353-3 - CITATION
THE STATE OF TEXAS**

To:

RDI XTRACT
SERVING ITS OHIO STATUTORY AGENT,
NEIL DESAI, 4350 GLENDALE MILFORD RD., STE. 250,
CINCINNATI OH, 45242.

GREETINGS:

You have been sued. You may employ an attorney. If you or your attorney do not file a written answer with the clerk who issued this citation by 10 o'clock a.m. of the Monday next following the expiration of twenty days after you were served this citation and petition, a default judgment may be taken against you. Your answer should be addressed to the clerk of the **14th District Court** at 600 Commerce Street, Ste. 101, Dallas, Texas 75202.

Said Plaintiff being MONEY SERVICES, INC.

Filed in said Court **28th day of August, 2020** against

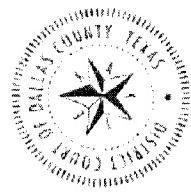
EXAMINATION MANAGEMENT SERVICES, INC., ET AL

For Suit, said suit being numbered **DC-20-12059**, the nature of which demand is as follows:
Suit on **OTHER (CIVIL)** etc. as shown on said petition, a copy of which accompanies this citation. If this citation is not served, it shall be returned unexecuted.

WITNESS: FELICIA PITRE, Clerk of the District Courts of Dallas, County Texas.
Given under my hand and the Seal of said Court at office this **2nd day of September, 2020**.

ATTEST: FELICIA PITRE, Clerk of the District Courts of Dallas, County, Texas

Courtney Rutledge
By **COURTNEY RUTLEDGE**, Deputy



ESERVE

CITATION

DC-20-12059

MONEY SERVICES, INC.

vs.
**EXAMINATION MANAGEMENT
SERVICES, INC., et al**

**ISSUED THIS
2nd day of September, 2020**

FELICIA PITRE
Clerk District Courts,
Dallas County, Texas

By: COURTNEY RUTLEDGE, Deputy

Attorney for Plaintiff
SUSAN EGELAND
FAEGRE DRINKER BIDDLE & REATH
1717 MAIN STREET SUITE 5400
DALLAS TX 75201-7367
469-357-2533
susan.egeland@faegredrinker.com

DALLAS COUNTY

SERVICE FEES

NOT PAID

OFFICER'S RETURN

Case No.: DC-20-12059

Court No. 14th District Court

Style: MONEY SERVICES, INC.

vs.

EXAMINATION MANAGEMENT SERVICES, INC., et al

Came to hand on the _____ day of _____, 20_____, at _____ o'clock _____. M. Executed at _____
within the County of _____ at _____ o'clock _____. M. on the _____ day of _____
20_____, by delivering to the within named

each, in person, a true copy of this Citation together with the accompanying copy of this pleading, having first endorsed on same date of delivery. The distance actually traveled by me in serving such process was _____ miles and my fees are as follows: To certify which witness my hand.

For serving Citation \$ _____
For mileage \$ _____ of _____ County.
For Notary \$ _____ By _____ Deputy

(Must be verified if served outside the State of Texas)

Signed and sworn to by the said _____ before me this _____ day of _____, 20_____.
to certify which witness my hand and seal of office.

Notary Public _____ County _____

**FORM NO. 353-3 - CITATION
THE STATE OF TEXAS**

To:

RDI CORPORATION
SERVED WITH PROCESS BY SERVING ITS OHIO
STATUTORY AGENT, GEORGE TREBBI,
4350 GLENDALE MILFORD RD., STE. 250,
CINCINNATI OH, 45242.

GREETINGS:

You have been sued. You may employ an attorney. If you or your attorney do not file a written answer with the clerk who issued this citation by 10 o'clock a.m. of the Monday next following the expiration of twenty days after you were served this citation and petition, a default judgment may be taken against you. Your answer should be addressed to the clerk of the **14th District Court** at 600 Commerce Street, Ste. 101, Dallas, Texas 75202.

Said Plaintiff being MONEY SERVICES, INC.

Filed in said Court **28th day of August, 2020** against

EXAMINATION MANAGEMENT SERVICES, INC., ET AL

By: COURTNEY RUTLEDGE, Deputy

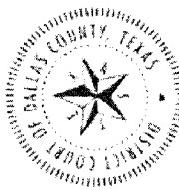
For Suit, said suit being numbered **DC-20-12059**, the nature of which demand is as follows:

Suit on **OTHER (CIVIL)** etc. as shown on said petition, a copy of which accompanies this citation. If this citation is not served, it shall be returned unexecuted.

WITNESS: FELICIA PITRE, Clerk of the District Courts of Dallas, County Texas.
Given under my hand and the Seal of said Court at office this 2nd day of September, 2020.

ATTEST: FELICIA PITRE, Clerk of the District Courts of Dallas, County, Texas

Courtney Rutledge
By COURTNEY RUTLEDGE, Deputy



Attorney for Plaintiff
SUSAN EGELAND
FAEGRE DRINKER BIDDLE & REATH
1717 MAIN STREET SUITE 5400
DALLAS TX 75201-7367
469-357-2533
susan.egeland@faegredrinker.com

DALLAS COUNTY
SERVICE FEES
NOT PAID

OFFICER'S RETURN

Case No.: DC-20-12059

Court No. 14th District Court

Style: MONEY SERVICES, INC.

vs.

EXAMINATION MANAGEMENT SERVICES, INC., et al

Came to hand on the _____ day of _____, 20_____, at _____ o'clock _____. M. Executed at _____
within the County of _____ at _____ o'clock _____. M. on the _____ day of _____
20_____, by delivering to the within named

each, in person, a true copy of this Citation together with the accompanying copy of this pleading, having first endorsed on same date of delivery. The distance actually traveled by
me in serving such process was _____ miles and my fees are as follows: To certify which witness my hand.

For serving Citation \$ _____
For mileage \$ _____ of _____ County.
For Notary \$ _____ By _____ Deputy

(Must be verified if served outside the State of Texas)

Signed and sworn to by the said _____ before me this _____ day of _____, 20_____.
to certify which witness my hand and seal of office.

Notary Public _____ County _____

**FORM NO. 353-3 - CITATION
THE STATE OF TEXAS**

To:

**EXAMINATION MANAGEMENT SERVICES, INC.
SERVING ITS REGISTERED AGENT FOR SERVICE: CT
CORPORATION 999 BRYAN STREET, SUITE 900, DALLAS, TEXAS 75201,**

GREETINGS:

You have been sued. You may employ an attorney. If you or your attorney do not file a written answer with the clerk who issued this citation by 10 o'clock a.m. of the Monday next following the expiration of twenty days after you were served this citation and petition, a default judgment may be taken against you. Your answer should be addressed to the clerk of the **14th District Court** at 600 Commerce Street, Ste. 101, Dallas, Texas 75202.

Said Plaintiff being **MONEY SERVICES, INC.**

Filed in said Court **28th day of August, 2020** against

EXAMINATION MANAGEMENT SERVICES, INC., ET AL

For Suit, said suit being numbered **DC-20-12059**, the nature of which demand is as follows:

Suit on **OTHER (CIVIL)** etc. as shown on said petition, a copy of which accompanies this citation. If this citation is not served, it shall be returned unexecuted.

WITNESS: FELICIA PITRE, Clerk of the District Courts of Dallas, County Texas.

Given under my hand and the Seal of said Court at office this 2nd day of September, 2020.

ATTEST: FELICIA PITRE, Clerk of the District Courts of Dallas, County, Texas

[Signature]
By _____, Deputy

COURTNEY RUTLEDGE

By _____, Deputy

**DALLAS COUNTY
SERVICE FEES
NOT PAID**

**ESERVE
CITATION**

DC-20-12059

MONEY SERVICES, INC.

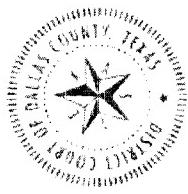
**vs.
EXAMINATION MANAGEMENT
SERVICES, INC., et al**

**ISSUED THIS
2nd day of September, 2020**

**FELICIA PITRE
Clerk District Courts,
Dallas County, Texas**

By: COURTNEY RUTLEDGE, Deputy

**Attorney for Plaintiff
SUSAN EGELAND
FAEGRE DRINKER BIDDLE & REATH
1717 MAIN STREET SUITE 5400
DALLAS TX 75201-7367
469-357-2533
susan.egeland@faegredrinker.com**



OFFICER'S RETURN

Case No.: DC-20-12059

Court No. 14th District Court

Style: MONEY SERVICES, INC.

vs.

EXAMINATION MANAGEMENT SERVICES, INC., et al

Came to hand on the _____ day of _____, 20_____, at _____ o'clock _____. M. Executed at _____
within the County of _____ at _____ o'clock _____. M. on the _____ day of _____
20_____, by delivering to the within named _____

each, in person, a true copy of this Citation together with the accompanying copy of this pleading, having first endorsed on same date of delivery. The distance actually traveled by me in serving such process was _____ miles and my fees are as follows: To certify which witness my hand.

For serving Citation	\$ _____
For mileage	\$ _____ of _____ County,
For Notary	\$ _____ By _____ Deputy

(Must be verified if served outside the State of Texas.)

Signed and sworn to by the said _____ before me this _____ day of _____, 20_____
to certify which witness my hand and seal of office.

Notary Public _____ County _____

CAUSE NO. DC-20-12059

MONEY SERVICES, INC.

卷之三

IN THE DISTRICT COURT

VS

**EXAMINATION MANAGEMENT
SERVICES, INC., ET AL.**

卷之三

14TH JUDICIAL DISTRICT

Defendant(s).

3
8

DALLAS COUNTY, TEXAS

RETURN OF SERVICE

Came to my hand on Wednesday, September 2, 2020 at 9:36 AM,
Executed at: 1999 BRYAN STREET, STE 900, DALLAS, TX 75201
within the county of DALLAS at 2:41 PM, on Wednesday, September 2, 2020,
by delivering to the within named:

EXAMINATION MANAGEMENT SERVICES, INC.

By delivering to its Registered Agent, CT CORPORATION SYSTEM
By personally delivering to its Authorized Agent, TERRI THONGSAVAT
a true copy of this

CITATION, PLAINTIFF'S ORIGINAL PETITION, APPLICATION FOR TEMPORARY RESTRAINING ORDER, AND APPLICATION FOR TEMPORARY AND PERMANENT INJUNCTIVE RELIEF, AND EXHIBITS

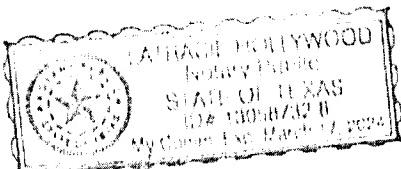
having first endorsed thereon the date of the delivery.

BEFORE ME, the undersigned authority, on this day personally appeared Adil Tadli who after being duly sworn on oath states: "My name is Adil Tadli. I am a person not less than eighteen (18) years of age and I am competent to make this oath. I am a resident of the State of Texas. I have personal knowledge of the facts and statements contained herein and aver that each is true and correct. I am not a party to nor related or affiliated with any party to this suit. I have no interest in the outcome of the suit. I have never been convicted of a felony or of a misdemeanor involving moral turpitude. I am familiar with the Texas Rules of Civil Procedure, and the Texas Civil Practice and Remedies Codes as they apply to service of process. I am certified by the Judicial Branch Certification Commission to deliver citations and other notices from any District, County and Justice Courts in and for the State of Texas in compliance with rule 103 and 501.2 of the TRCP."

By:

Adil Tadli - PSC 1206 - Exp 05/31/22
served@specialdelivery.com

Subscribed and Sworn to by Adil Tadli, Before Me, the undersigned authority, on this 8th day of September, 2020.



Me, the undersigned authority, on this 8th day of
Laticia Hall
Notary Public in and for the State of Texas

**FORM NO. 353-3 - CITATION
THE STATE OF TEXAS**

To: EXAMINATION MANAGEMENT SERVICES, INC.
SERVING ITS REGISTERED AGENT FOR SERVICE: CT
CORPORATION 1999 BRYAN STREET, SUITE 900, DALLAS, TEXAS 75201,

GREETINGS:

You have been sued. You may employ an attorney. If you or your attorney do not file a written answer with the clerk who issued this citation by 10 o'clock a.m. of the Monday next following the expiration of twenty days after you were served this citation and petition, a default judgment may be taken against you. Your answer should be addressed to the clerk of the **14th District Court** at 600 Commerce Street, Ste. 101, Dallas, Texas 75202.

Said Plaintiff being MONEY SERVICES, INC.

Filed in said Court **28th day of August, 2020** against

EXAMINATION MANAGEMENT SERVICES, INC., ET AL

For Suit, said suit being numbered **DC-20-12059**, the nature of which demand is as follows:
Suit on **OTHER (CIVIL)** etc. as shown on said petition. a copy of which accompanies this citation. If this citation is not served, it shall be returned unexecuted.

WITNESS: FELICIA PITRE, Clerk of the District Courts of Dallas, County Texas.
Given under my hand and the Seal of said Court at office this **2nd day of September, 2020**.

ATTEST: FELICIA PITRE, Clerk of the District Courts of Dallas, County, Texas
[Signature] _____, Deputy
By _____ COURTNEY RUTLEDGE



<u>E.SERVE</u>	<u>CITATION</u>	<u>MONEY SERVICES, INC.</u>
		vs. EXAMINATION MANAGEMENT SERVICES, INC., et al
		ISSUED THIS 2nd day of September, 2020
		FELICIA PITRE Clerk District Courts, Dallas County, Texas
		By: COURTNEY RUTLEDGE
		Attorney for Plaintiff SUSAN EGELAND FAEGRE DRINKER BIDDLE & REATH 1717 MAIN STREET SUITE 5400 DALLAS TX 75201-7367 469-357-2533 susan.egeland@faegredrinker.com
		DALLAS COUNTY
		SERVICE FEES
		NOT PAID

OFFICER'S RETURN

Case No. : DC-20-12059

Court No. 14th District Court

Style: MONEY SERVICES, INC.

vs.

EXAMINATION MANAGEMENT SERVICES, INC., et al

Came to hand on the _____ day of _____, 20_____, at _____ o'clock _____ M. Executed at _____
within the County of _____ at _____ o'clock _____. M. on the _____ day of _____
20 _____, by delivering to the within named _____

each, in person, a true copy of this Citation together with the accompanying copy of this pleading, having first endorsed on same date of delivery. The distance actually traveled by
me in serving such process was _____ miles and my fees are as follows: To certify which witness my hand.

For serving Citation \$ _____
for mileage \$ _____
For Notary \$ _____
By _____ Deputy _____
(Must be verified if served outside the State of Texas.)

Signed and sworn to by the said _____ before me this _____ day of _____, 20_____.
to certify which witness my hand and seal of office.

Notary Public _____ County _____

CAUSE NO. DC-20-12059

MONEY SERVICES, INC. § IN THE DISTRICT COURT
Plaintiff(s), §
VS. § 14TH JUDICIAL DISTRICT
EXAMINATION MANAGEMENT §
SERVICES, INC., ET AL. §
Defendant(s). § DALLAS COUNTY, TEXAS

RETURN OF SERVICE

Came to my hand on Wednesday, September 2, 2020 at 9:36 AM,
Executed at: 1999 BRYAN STREET, STE 900, DALLAS, TX 75201
within the county of DALLAS at 2:41 PM, on Wednesday, September 2, 2020,
by delivering to the within named:

EMSI HOLDING COMPANY

By delivering to its Registered Agent, CT CORPORATION SYSTEM
By personally delivering to its Authorized Agent, TERRI THONGSAVAT
a true copy of this

CITATION, PLAINTIFF'S ORIGINAL PETITION, APPLICATION FOR TEMPORARY RESTRAINING ORDER, AND APPLICATION FOR TEMPORARY AND PERMANENT INJUNCTIVE RELIEF, AND EXHIBITS

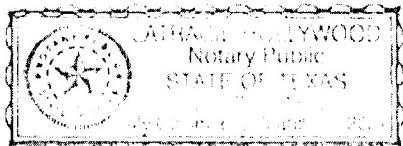
having first endorsed thereon the date of the delivery.

BEFORE ME, the undersigned authority, on this day personally appeared **Adil Tadli** who after being duly sworn on oath states: "My name is **Adil Tadli**. I am a person not less than eighteen (18) years of age and I am competent to make this oath. I am a resident of the State of Texas. I have personal knowledge of the facts and statements contained herein and aver that each is true and correct. I am not a party to nor related or affiliated with any party to this suit. I have no interest in the outcome of the suit. I have never been convicted of a felony or of a misdemeanor involving moral turpitude. I am familiar with the Texas Rules of Civil Procedure, and the Texas Civil Practice and Remedies Codes as they apply to service of process. I am certified by the Judicial Branch Certification Commission to deliver citations and other notices from any District, County and Justice Courts in and for the State of Texas in compliance with rule 103 and 501.2 of the TRCP."

By: _____

Adil Tadli - PSC 1206 - Exp 05/31/22
served@specialdelivery.com

Subscribed and Sworn to by Adil Tadli, Before Me, the undersigned authority, on this 5th day of September, 2020.



e, the undersigned authority, on this 8th day

Latrice Hollywood
Notary Public in and for the State of Texas

**FORM NO. 353-3 - CITATION
THE STATE OF TEXAS**

To:

EMSI HOLDING COMPANY
SERVING ITS REGISTERED AGENT FOR SERVICE
CT CORPORATION 1999 BRYAN STREET, SUITE 900,
DALLAS, TEXAS 75201,

GREETINGS:

You have been sued. You may employ an attorney. If you or your attorney do not file a written answer with the clerk who issued this citation by 10 o'clock a.m. of the Monday next following the expiration of twenty days after you were served this citation and petition, a default judgment may be taken against you. Your answer should be addressed to the clerk of the 14th District Court at 600 Commerce Street, Ste. 101, Dallas, Texas 75202.

Said Plaintiff being MONEY SERVICES, INC.

Filed in said Court 28th day of August, 2020 against

EXAMINATION MANAGEMENT SERVICES, INC., ET AL

For Suit, said suit being numbered DC-20-12059, the nature of which demand is as follows:
Suit on **OTHER (CIVIL)** etc. as shown on said petition, a copy of which accompanies this citation. If this citation is not served, it shall be returned unexecuted.

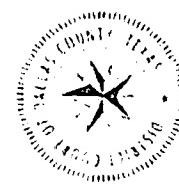
WITNESS: FELICIA PITRE, Clerk of the District Courts of Dallas, County Texas.

Given under my hand and the Seal of said Court at office this 2nd day of September, 2020.

ATTEST: FELICIA PITRE, Clerk of the District Courts of Dallas, County, Texas

[Signature]
By _____, Deputy

COURTNEY RUTLEDGE



<u>ESERVE</u>	<u>CITATION</u>
DC-20-12059	
	MONEY SERVICES, INC. vs. EXAMINATION MANAGEMENT SERVICES, INC., et al
	ISSUED THIS 2nd day of September, 2020
	FELICIA PITRE Clerk District Courts, Dallas County, Texas
	By: COURTNEY RUTLEDGE, Deputy
	Attorney for Plaintiff SUSAN EGELAND FAEGRE DRINKER BIDDLE & REATH 1717 MAIN STREET SUITE 5400 DALLAS TX 75201-7367 susan.egeland@faegredrinker.com
	DALLAS COUNTY
	SERVICE FEES
	NOT PAID

OFFICER'S RETURN

Case No. : DC-20-12059

Court No. 14th District Court

Style: MONEY SERVICES, INC.

vs.

EXAMINATION MANAGEMENT SERVICES, INC., et al

Came to hand on the _____ day of _____, 20_____, at _____ o'clock _____ M. Executed at _____
within the County of _____ at _____ o'clock _____. M. on the _____ day of _____
20_____, by delivering to the within named _____

each, in person, a true copy of this Citation together with the accompanying copy of this pleading, having first endorsed on same date of delivery. The distance actually traveled by
me in serving such process was _____ miles and my fees are as follows: To certify which witness my hand.

For serving Citation \$ _____
For mileage \$ _____
of _____ County.
By _____ Deputy
For Notary \$ _____

(Must be verified if served outside the State of Texas.)

Signed and sworn to by the said _____ before me this _____ day of _____, 20_____.
to certify which witness my hand and seal of office.

Notary Public _____ County _____

CAUSE NO. DC-20-12059**MONEY SERVICES, INC.****Plaintiff,****v.****EXAMINATION MANAGEMENT
SERVICES, INC.. EMSI HOLDING
COMPANY, RDI XTRACT, LLC, RDI
CORPORATION****Defendants.****IN THE DISTRICT COURT OF****DALLAS COUNTY, TEXAS****14th JUDICIAL DISTRICT COURT****MOTION TO TRANSFER PURSUANT TO LOCAL RULE 1.06**

1. Plaintiff Money Services, Inc. filed its Original Petition, Application for Temporary Restraining Order, and Application for Temporary and Permanent Injunctive Relief on August 28, 2020. This case is in its inception, and Plaintiff is in the process of formally serving Defendants.
2. At the time of filing, Plaintiff included a Certification pursuant to Local Rule 1.06 stating:

Pursuant to Local Rule 1.06, the undersigned counsel informs the Court that there exists a related case filed on July 27, 2020 titled *The Savings Bank Mutual Life Insurance Company of Massachusetts v. Examination Management Services, Inc. and EMSI Holding Company*, In the 68th District Court of Dallas County, Texas, Cause No. DC-20-10143. MSI advises the Court that transfer of this case to the 68th District Court "would facilitate orderly and efficient disposition of the litigation" as contemplated by Local Rule 1.06.

3. However, the case was filed in the 14th Judicial District Court of Dallas County.
4. Because the matters at issue in *The Savings Bank Mutual Life Insurance Company of Massachusetts v. Examination Management Services, Inc. and EMSI Holding Company*, In the 68th District Court of Dallas County, Texas, Cause No. DC-20-10143, are substantially related to those at issue in this case, Plaintiff respectfully requests transfer of DC-20-12059 to this 68th

District Court. In addition, there are two additional related matters involving the same parties that were also recently transferred to the 68th District Court on the plaintiff's motions: (1) *John Hancock Life Insurance Company (U.S.A.) v. RDI Xtract, LLC, et al.*, Cause No. DC-20-10780;¹ and (2) *John Hancock Life Insurance Company (U.S.A.) v. Examination Management Services, Inc., et al.*, Cause No. DC-20-10581.

5. Plaintiff believes transfer is required by Local Rule 1.06.

Respectfully submitted,

/s/ Susan Egeland

Susan Egeland
State Bar No. 24040854
susan.egeland@faegredrinker.com
FAEGRE DRINKER BIDDLE & REATH LLP
1717 Main Street, Suite 5400
Dallas, TX 75201
Telephone: (469) 357-2500
Facsimile: (469) 327-0860

ATTORNEY FOR MONEY SERVICES, INC.

¹ This case has since been removed to the Northern District of Texas, Dallas Division.

CERTIFICATE OF CONFERENCE

In deference to Local Rule 2.07, but given the nature of the relief (an Original Petition with TRO), Plaintiff states as follows:

“An emergency exists of such nature that further delay would cause irreparable harm to the movant, as follows:”

This case is in its inception, and Plaintiff is in the process of formally serving Defendants. Therefore, there is no counsel of record for any Defendant. Plaintiff will advise the presumed representatives for Defendants at least two hours before the TRO application and proposed order are to be presented to the Court for decision (Local Rule 2.02). The presumed representatives include: the EMSI Board (Board@emsinet.com), Troy Phillips, a member of the EMSI Board (tphillips@bpoc.com), Kamette Myers, President of RDI Xtract (kmyers@rdixtract.com), an Mike Coles (mikec@colesfirm.com), counsel for RDI Xtract and RDI Corporation.

Based on course of dealing, Plaintiff reasonably assumes that the presumed representatives of EMSI will not respond regarding opposition/non-opposition to the Motion to Transfer. Plaintiff reasonably assumes that the presumed representatives of RDI and RDI Xtract will not oppose the Motion to Transfer.

Plaintiff will seek to have its Motion to Transfer heard in the 68th District Court immediately prior to the hearing on its TRO.

/s/ Susan E. Egeland
SUSAN E. EGELAND

CERTIFICATE OF SERVICE

This is to certify that a true and correct copy of the foregoing document has been forwarded to all counsel of record via eFile Texas on September 3, 2020.

/s/ Susan E. Egeland
SUSAN E. EGELAND

Automated Certificate of eService

This automated certificate of service was created by the efiling system. The filer served this document via email generated by the efiling system on the date and to the persons listed below. The rules governing certificates of service have not changed. Filers must still provide a certificate of service that complies with all applicable rules.

Danette Dykema on behalf of Susan Egeland
Bar No. 24040854
Danette.dykema@faegredrinker.com
Envelope ID: 45946892
Status as of 9/3/2020 3:58 PM CST

Case Contacts

Name	BarNumber	Email	TimestampSubmitted	Status
Susan Elizabeth Egeland	24040854	susan.egeland@faegredrinker.com	9/3/2020 10:59:55 AM	SENT
Danette Dykema		Danette.dykema@faegredrinker.com	9/3/2020 10:59:55 AM	SENT

CAUSE NO. DC-20-12059

MONEY SERVICES, INC.

Plaintiff,

v.

**EXAMINATION MANAGEMENT
SERVICES, INC.. EMSI HOLDING
COMPANY, RDI XTRACT, LLC, RDI
CORPORATION**

Defendants.

IN THE DISTRICT COURT OF

DALLAS COUNTY, TEXAS

14th JUDICIAL DISTRICT COURT

ORDER GRANTING MOTION TO TRANSFER PURSUANT TO LOCAL RULE 1.06

Having considered Money Services, Inc.'s Motion to Transfer Pursuant to Local Rule 1.06,

IT IS NOW, ORDERED, ADJUDGED AND DECREED that Cause No. DC-20-12059 is transferred from the 14th Judicial District Court to the 68th Judicial District Court for all future proceedings.

SIGNED this _____, 2020.

PRESIDING JUDGE

Automated Certificate of eService

This automated certificate of service was created by the efiling system. The filer served this document via email generated by the efiling system on the date and to the persons listed below. The rules governing certificates of service have not changed. Filers must still provide a certificate of service that complies with all applicable rules.

Danette Dykema on behalf of Susan Egeland
Bar No. 24040854
Danette.dykema@faegredrinker.com
Envelope ID: 45946892
Status as of 9/3/2020 3:58 PM CST

Case Contacts

Name	BarNumber	Email	TimestampSubmitted	Status
Danette Dykema		Danette.dykema@faegredrinker.com	9/3/2020 10:59:55 AM	SENT
Susan Elizabeth Egeland	24040854	susan.egeland@faegredrinker.com	9/3/2020 10:59:55 AM	SENT

Civil Case Cover Sheet
In The District Court
of Dallas County, Texas

September 04, 2020

SUSAN EGELAND
FAEGRE DRINKER BIDDLE & REATH
1717 MAIN STREET SUITE 5400
DALLAS TX 75201-7367

IN RE: DC-20-12059
MONEY SERVICES, INC. vs. EXAMINATION MANAGEMENT SERVICES, INC., et al

PLEASE SEE ATTACHMENT(S): ORDER TRANSFER

Attorneys update your information at:
<https://www.dallascounty.org/government/district-clerk/attorney-form.php>

SUSAN EGELAND
FAEGRE DRINKER BIDDLE &
REATH
1717 MAIN STREET SUITE 5400
DALLAS TX 75201-7367

CAUSE NO. DC-20-12059

MONEY SERVICES, INC.

Plaintiff,

v.

**EXAMINATION MANAGEMENT
SERVICES, INC., EMSI HOLDING
COMPANY, RDI XTRACT, LLC, RDI
CORPORATION**

Defendants.

IN THE DISTRICT COURT OF

DALLAS COUNTY, TEXAS

14th JUDICIAL DISTRICT COURT

ORDER GRANTING MOTION TO TRANSFER PURSUANT TO LOCAL RULE 1.06

Having considered Money Services, Inc.'s Motion to Transfer Pursuant to Local Rule 1.06,

IT IS NOW, ORDERED, ADJUDGED AND DECREED that Cause No. DC-20-12059 is transferred from the 14th Judicial District Court to the 68th Judicial District Court for all future proceedings.

SIGNED this

, 2020.

PRÉSIDING JUDGE

DC-20-12059

CAUSE NO. _____

MONEY SERVICES, INC.

Plaintiff,

v.

**EXAMINATION MANAGEMENT
SERVICES, INC., EMSI HOLDING
COMPANY, RDI XTRACT, LLC, RDI
CORPORATION**

Defendants.

IN THE DISTRICT COURT OF

DALLAS COUNTY, TEXAS

JUDICIAL DISTRICT COURT

TEMPORARY RESTRAINING ORDER

After considering Plaintiff's Original Petition, Application for Temporary Restraining Order, and Application for Temporary and Permanent Injunctive Relief, and the pleadings, declarations, and arguments of counsel, the Court finds and concludes that there is sufficient evidence that, if it does not enter this Temporary Restraining Order, there is a serious and imminent threat that Plaintiff Money Services, Inc. ("MSI") will suffer irreparable harm from the actions of Examination Management Services, Inc., EMSI Holding Company, RDI Xtract LLC ("RDI Xtract") and RDI Corporation (collectively, "Defendants") with respect to the business information of MSI. Specifically, the verified allegations of MSI establish that (1) EMSI transferred control of data servers that store records created and maintained by Examination Management Services, Inc. (EMSI) on behalf of MSI, including MSI's Proprietary Information, to RDI Xtract without MSI's authorization; (2) MSI is the exclusive owner of its Proprietary Information; (3) EMSI and RDI Xtract have refused to return and subsequently destroy MSI's Proprietary Information, which RDI Xtract and EMSI are obligated to do upon request; (4) MSI faces immediate and direct damage and irreparable harm with regard to its business if its

Proprietary Information is not safely returned or if any third parties gain access to its Proprietary Information.

The Court has been advised that at least two hours' notice of this application for a Temporary Restraining Order has been provided to Defendants. The Court finds that an ex parte order and hearing without further notice to Defendants is warranted because it appears that MSI may have already suffered irreparable injury, loss, or damage and that there is a threat of continuing irreparable harm, loss, or damage to MSI if a restraining order is not granted as requested, to wit, the risk of unauthorized disclosure of MSI's records to RDI Xtract or other third parties and permanent loss of MSI's Proprietary Information, which is important for MSI's ongoing business operations.

Accordingly, the Court hereby orders that Defendants, their directors, officers, employees, agents, representatives, and counsel, and all other persons and entities in active concert or participation with any of them, are and shall be enjoined and restrained from:

- a. Failing to protect and preserve MSI's Proprietary Information;
- b. Accessing, or allowing any other third party, to access or otherwise take physical possession of any data servers prior to the destruction of MSI's Proprietary Information, without MSI's advance, written consent;
- c. Denying, interfering or otherwise refusing to cooperate with MSI's rights under the Contract with respect to MSI's Proprietary Information, including its right to audit and access its data or any other documents or information to which it is entitled, including the servers on which that data is stored.

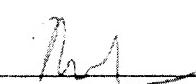
The Court further orders Defendants jointly and severally to (i) immediately return MSI's Proprietary Information on behalf of EMSI in a format acceptable to MSI; (ii) securely destroy MSI's Proprietary Information on behalf of EMSI and provide an affidavit attesting to the same; (iii) provide or otherwise arrange for MSI to have full and complete access to the servers that contain MSI's Proprietary Information, subject to the Parties' existing confidentiality agreements,

for the purpose of auditing RDI's and EMSI's privacy obligations under the Contract and the law and to ensure the data's safe destruction pursuant to the Court's order; and (iv) provide a copy of the asset sale agreement and any other agreements related to the sale of the data servers. The Court further orders Defendants to cooperate and provide reasonable assistance to MSI in connection with accessing the servers for the purpose of auditing RDI's and EMSI's privacy obligations and to ensure the data's safe return and destruction pursuant to the Court's order.

The Court sets bond in the amount of \$ 500.

Unless it is extended in writing before September 11, 2020, by further written order of this Court, this Temporary Restraining Order expires on its own terms at 11:59 on September 11, 2020. *Temporary Restraining Order will expire on September 11, 2020 at 11:59.*
IT IS SO ORDERED.

SIGNED at 9:00 a.m. on this 11 day of August, 2020.



JUDGE PRESIDING



**FELICIA PITRE, DISTRICT CLERK
REGISTRY DEPOSIT INFORMATION SHEET
FOR MINORS, INTERPLEADERS & CASH BONDS**

CASE # DC 20-12059-C AMOUNT 500.00

BOND TYPE T.R.O. CHECK # _____
AMOUNT _____
CHECK # _____

CASE STYLE Money Services Inc. vs. Examination Management

ARE THESE FUNDS TO BE INVESTED? YES NO

TAX ID #. or SOC. SEC. # _____
(TRUST MUST HAVE A COPY TO HAVE FUNDS INVESTED)

PARTY NAME or MINOR'S NAME _____
(REQUIRED)

MINOR'S DATE OF BIRTH _____
(REQUIRED)

MINOR'S PARENT OR GUARDIAN NAME & ADDRESS, PH. # & DRIVERS LICENSE # _____

PH.#	D.L.#
<small>(REQUIRED)</small>	<small>(REQUIRED)</small>

PLAINTIFF ATTY. Susan Egeland DEFENDANT ATTY. or GAL. _____
ADDRESS 1717 Main Street
Suite 500
Dallas, TX 75201

PHONE # 214 557 3403 PHONE # _____

NOTE: REGISTRY FUNDS WILL BE INVESTED ONLY IF A COPY OF SOCIAL SECURITY OR TAX ID NUMBER IS PROVIDED.

TYPES OF INTEREST BEARING ACCOUNTS ALLOWED PER SECTION 117.053 OF THE LOCAL GOVERNMENT CODE: INTERLOCAL INVESTMENT POOLS, LOCAL INTEREST BEARING DEPOSITS THAT ARE FDIC INSURED (CD, MMA'S, SAVINGS ACCOUNTS), UNITED STATES TREASURY BILLS AND NO LOAD MONEY MARKET MUTUAL FUNDS. ALL OF THESE INTEREST BEARING VEHICLES ARE SUBJECT TO THE STRICT GUIDELINES SET FORTH IN SECTION 117.053 OF THE LOCAL GOVERNMENT CODE. *A FEE OF 10% OF THE INTEREST EARNED WILL BE ASSESSED AT THE TIME OF WITHDRAWAL ON INVESTED ACCOUNTS PER SECTION 117.122 OF THE LOCAL GOVERNMENT CODE.

IT IS DISTRICT CLERK POLICY REGARDING FINAL JUDGMENTS TO WAIT 30 DAYS TO DISPERSE REGISTRY FUNDS. THIS IS DUE TO THE FACT THAT THE CASE CAN BE APPEALED WITHIN 30 DAYS. THE EXCEPTION TO THIS IS: AGREED FINAL JUDGMENTS, OR THE FINAL JUDGMENT CONTAINS WORDING ORDERING THE DISTRICT CLERK TO FORGO THE 30 DAY WAIT. ALSO A NON-JUDGMENT ORDER OF THE COURT WILL SUFFICE IN ORDER TO RELEASE COURT REGISTRY FUNDS IMMEDIATELY. THE DISTRICT CLERK TRUST OFFICE WILL ALSO WAIT TO DISBURSE FUNDS FROM THE COURT'S REGISTRY IF THE DEPOSIT WAS RECENTLY MADE BY CHECK. THIS WILL ALLOW THE TRUST OFFICE ENOUGH TIME TO SEE IF THE CHECK HAS CLEARED.

IT IS THE RESPONSIBILITY OF THE ATTORNEYS OF RECORD TO SUBMIT A COURT ORDER TO REQUEST A DISBURSEMENT OF ANY MONIES DEPOSITED IN LIEU OF BOND OR INTERPLEADER ACTIONS AND TIMELY NOTIFY THE TRUST DEPARTMENT OF ANY INVESTMENT OR WITHDRAWAL. IF YOU WIRE TRANSFER FUNDS INTO THE COURT'S REGISTRY, THEN YOU NEED TO FILL OUT A REGISTRY DEPOSIT FORM LOCATED UNDER DOWNLOADABLE FORMS ONLINE UNDER THE DISTRICT CLERK'S WEB SITE www.dallascounty.org/department/districtclerk/districtclerk_index.html AND SUBMIT A COPY TO THE D.C. TRUST OFFICE.

SIGNATURE [Signature] DATE 9-4-2020

OFFICIAL RECEIPT
DALLAS COUNTY OFFICIAL RECEIPT FELICIA PITRE, DISTRICT CLERK

Payor

EGELAND, SUSAN
 FAEGRE, DRINKER BIDDLE & REATH
 1717 MAIN STREET SUITE 5400
 DALLAS, TX 75201-7367

Receipt No.

54437-2020-DCLK

Transaction Date
 09/4/2020

Description	Amount Paid
On Behalf Of MONEY SERVICES, INC. DC-20-12059 MONEY SERVICES, INC. vs. EXAMINATION MANAGEMENT SERVICES, INC., et al Bond Account	
CASH BOND DEPOSIT (CIVIL)	500.00
SUBTOTAL	500.00
Convenience Fee	14.50
PAYMENT TOTAL	514.50
VERIFONE CREDIT CARD (Ref #2955568711)	
Tendered	500.00
Total Tendered	500.00
Change	0.00
09/04/2020	Cashier
03:49 PM	Station DC142
	Audit
	63601478

OFFICIAL RECEIPT

DC-20-12059

Money Services Inc.

vs.

Examination Management
Services, Inc., et al

T.R.O. Cash Bond

Belinda Hernandez
DEPUTY

29 SEP -4 PM 3:44

Payer
THE COLES FIRM PC

Receipt N
55902-2020-DCL

Transaction Da
09/11/2020

Description	Amount Paid
Miscellaneous Payment	
COPIES AND POSTAGE FEES	174.00
SUBTOTAL	174.00
PAYMENT TOTAL	174.00
CHECK (Ref #3507) Tendered	174.00
Total Tendered	174.00
Change	0.00
09/11/2020	Cashier
03:26 PM	Station DC46
	Audit
	63609243

REPRINTED RECEIPT